IPSec VPN Client TheGreenBow

User Guide

Contact: support@thegreenbow.com

Website: www.thegreenbow.com

Property of TheGreenBow© - Sistech SA 2000-2007

TheGreenBow IPSec VPN Client - User Guide

Property of TheGreenBow© - Sistech SA 2000-2007

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: January 2007 in San Francisco.

Table of Contents

Part I Introducing TheGreenBow IPSec VPN Client 2

1 What is TheGreenBow IPSec VPN Client ? 2
2 Multi VPN Gateway solution 2
3 Linux Appliance Support 2
4 TheGreenBow IPSec VPN Client Features 2
5 OEM and Software rebranding 4

Part II Installing TheGreenBow IPSec VPN Client 6

1 Software Installation 6
2 Software Evaluation 6
3 Temporary Software License 7
4 Software Activation 9
Software Activation Wizard 9
Step 1 of 2: Enter License Number 9
Step 2 of 2: Online Activation 10
Activation Troubleshooting 10
5 Software Upgrade 11
6 Software Uninstallation 12

Part III Quick HowTo's 14

1 HowTo Open VPN tunnel? 14
2 HowTo Troubleshoot VPN tunnel? 14
3 HowTo import with double click on VPN Configuration icon? 14

Part IV Navigating the User Interface 17

1 User interface elements 17
2 System Tray Icon 18
3 Keyboard Shortcuts 18
4 Configuration Panel 19
Main Menus 19
Status Bar 20
Windows "About" 20
Access Control & Hidden Interface 21
Wizards 22
Preferences 23
5 Connection Panel 23

Part V Connection Panel 26

1 Connection Panel basics 26
2 More info about Connections 27

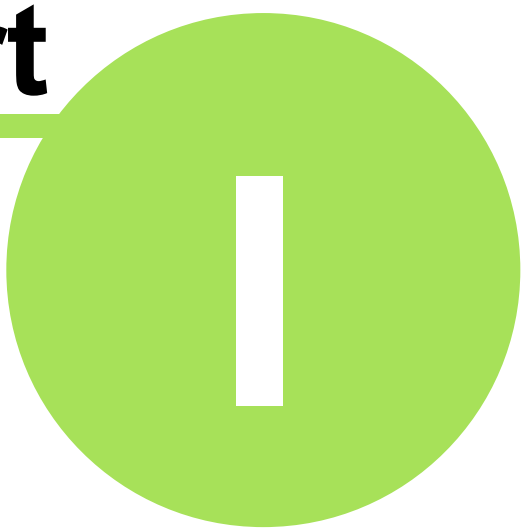
Part VI VPN Configuration 30

1 Configuration Wizard 30
Three step Configuration Wizard 30
Step 1 of 3: Choice of remote equipment 30
Step 2 of 3: VPN tunnel parameters 31
Step 3 of 3: Summary 32
2 VPN Tunnel Configuration 32
How to create a VPN Tunnel ? 32
Multiple Authentication or IPSec Configuration Phase 33
Advanced Features 33
3 Authentication or Phase 1 33
What is Phase 1 ? 33
Phase 1 Settings Description 34
Phase1 Advanced Settings Description 35
4 IPSec Configuration or Phase 2 37
What is Phase 2 ? 37
Phase 2 Settings Description 38
Phase2 Advanced Settings Description 39
Script configuration 40
5 Global Parameters 41
Global Settings Description 41
6 VPN Tunnel View 42
How to view opened tunnels ? 42
7 USB Mode 43
What is USB Mode ? 43
How to set USB Mode ? 43
How to enable a new USB Stick ? 44
How to automatically open tunnels when an USB Stick is plugged in ? 45
8 Certificate Management 45
Certificate Management overview 45
How to configure IPSec VPN Client with PKCS#12 Certificates 46
How to configure IPSec VPN Client with PEM Certificates 47
Smart Card and Token Management 49
How to configure a tunnel with Certificates from a SmartCard 49
How to use a tunnel with Certificates from a SmartCard 51
SmartCard Troubleshooting 51
9 Configuration Management 52
Import or Export VPN Configuration via menu 52
Embed your own VPN Configuration into IPSec VPN Client Setup 53
Default VPN Configuration 53
Part VII Deployment 55
1 Embedded VPN Configuration 55
2 Setup options 55
Setup option overview 55
Setup option for GUI mode 55
Setup option for GUI mode access control 55
Setup option for systray menu items 56
Other Setup options 56
3 Command line 57
Command line options 57
Stopping IPSec VPN Client: option "/stop" 57
Import VPN Configuration options 57

Property of TheGreenBow© - Sistech SA 2000-2007

Part VIII Console and Logs 60
1 Console Windows 60
2 Console Filters 61
Part IX Software Localization 63
Part X Contacts 65
Index 66

Part



Introducing TheGreenBow IPSec VPN Client

1 Introducing TheGreenBow IPSec VPN Client

1.1 What is TheGreenBow IPSec VPN Client ?

TheGreenBow IPSec VPN Client is an IPSec VPN software for all Windows versions that allows to establish secure connections over the Internet usually between a remote worker and the Corporate Intranet. IPSec is the most secure way to connect to the enterprise as it provide strong user authentication, strong tunnel encryption with ability to cope with existing network and firewall settings.
TheGreenBow IPSec VPN Client is the result of many years of experience in network security and Windows network driver development, as well as extensive research in related areas.
The IPSec VPN Client completes our range of network security products and like all our products is extremely easy to use and to install.

1.2 Multi VPN Gateway solution

TheGreenBow strategy is to support as many VPN gateway and appliance vendors as possible, available right now on the market in order to offer a true multi vendor solution to its customers. New IPSec VPN gateways or appliances are tested in our labs. The list of certified gateways is available on our web site and is increasing daily, thus do not hesitate to regularly check for new certified VPN gateways.

1.3 Linux Appliance Support

TheGreenBow supports several implementations of Linux IPSec VPN like StrongS/WAN and FreeS/WAN. Therefore TheGreenBow IPSec VPN Client is compatible with most of the IPSec routers/appliances based on those Linux implementations. We will support more Linux implementations in the future. The list of supported Linux VPN appliance is available on our website.

1.4 TheGreenBow IPSec VPN Client Features

Windows supported versions	Win98 ,Me, NT, Win2000, WinXP
Connection Mode	It operates as a peer-to-peer VPN as well as "point – to – multiple" mode, without a gateway or server. All connections types like Dial up, DSL, Cable, GSM/GPRS and WiFi are supported. Allow IP Range networking. It can run in an RDP session (Remote Desktop connection).
Tunneling Protocol	Full IKE support: Our IKE implementation is based on the OpenBSD 3.1 implementation (ISAKMPD), thus providing best compatibility with existing IPSec routers and gateways. Full IPSec support: • Main mode and Aggressive mode • MD5 and SHA hash algorithms • Change IKE port

Property of TheGreenBow© - Sistech SA 2000-2007

NAT Traversal	NAT Traversal Draft 1 (enhanced), Draft 2 and 3 (full implementation) • Including NAT_OA support • Including NAT keepalive • Including NAT T Aggressive Mode Forced NAT-Traversal mode.
Encryption	It provides 3DES, DES and AES 128/192/256bits encryption. Additional capabilities like DH1536, DH2048 groups are also provided.
User Authentication	• X-AUTH support • PreShared keying and X509 Certificates support. It is compatible with most of the currently available IPSec gateways • Support of Group 1, 2, 5 and 14 (i.e. 768, 1024, 1536 and 2048) • Flexible Certificate support (PEM, PKCS12, ...). PKCS#12 certificates can be directly imported from the user interface. • Ability to configure one Certificate per tunnel. • Hybrid Authentication Method support • SmartCards support
Dead Peer Detection (DPD)	DPD is an Internet Key Exchange (IKE) extension (i.e. RFC3706) for detecting a dead IKE peer.
Redundant Gateway	Redundant Gateway can offer to remote users a highly reliable secure connection to the corporate network. Redundant Gateway feature allows TheGreenBow VPN Client to open an IPSec tunnel with an alternate gateway in case the primary gateway is down or not responding.
Mode Config	"Mode Config" is an Internet Key Exchange (IKE) extension that enables the IPSec VPN gateway to provide LAN configuration to the remote user's machine (i.e. IPSec VPN Client). With Config-Mode the end-user is able to address all servers on the remote network by using their network name (e.g. //myserver/marketing/budget) instead of their IP Address.
USB Stick	VPN configurations and security elements (certificates, preshared key,…) can be saved into an USB Stick in order to remove security information (e.g.authentication) from the computer. Automatically open and close tunnels when plugging in or removing USB Stick.
Smart Card and Token	TheGreenBow IPSec VPN Client can read Certificates from Smart Cards to make full use of existing corporate ID card or employee cards that may carry Digital credentials.
Log console	All phase messages are logged for testing or staging purposes, and multiple filters (10) allows to easily narrow the view on specific aspects.
Flexible User Interface	Silent install and invisible graphical interface allow IT managers to deploy solutions while preventing user to misuse configurations. Tiny Connection Panel and VPN Configuration Panel can be available to end-users separately with access control. Drag & drop VPN Configurations into the IPSec VPN Client. Multiple keyboard shortcuts to easily navigate the IPSec VPN Client
Scripts	Scripts or applications can be launched automatically on several events (e.g. before and after a tunnel opens, before and after a tunnel is closed).
Configuration Management	User Interface and Command Line. Password protected VPN configuration file. Specific VPN configuration file can be provided within the setup. Embedded default VPN Configuration to test and debug with online TheGreenBow servers.
Live update	Incremental install allows to replace encryption or authentication modules with new releases. This works in addition to the live update feature which allows to update software from a central server.

Property of TheGreenBow© - Sistech SA 2000-2007

Licensing	Lifetime, Temporary, Release based Licensing are available.

1.5 OEM and Software rebranding

Our offer is specially designed to target OEM clients and System Integrators. We provide a fully functional VPN Client solution to complete existing offers. Our IPSec VPN Client can be re-branded.

Property of TheGreenBow© - Sistech SA 2000-2007

Part

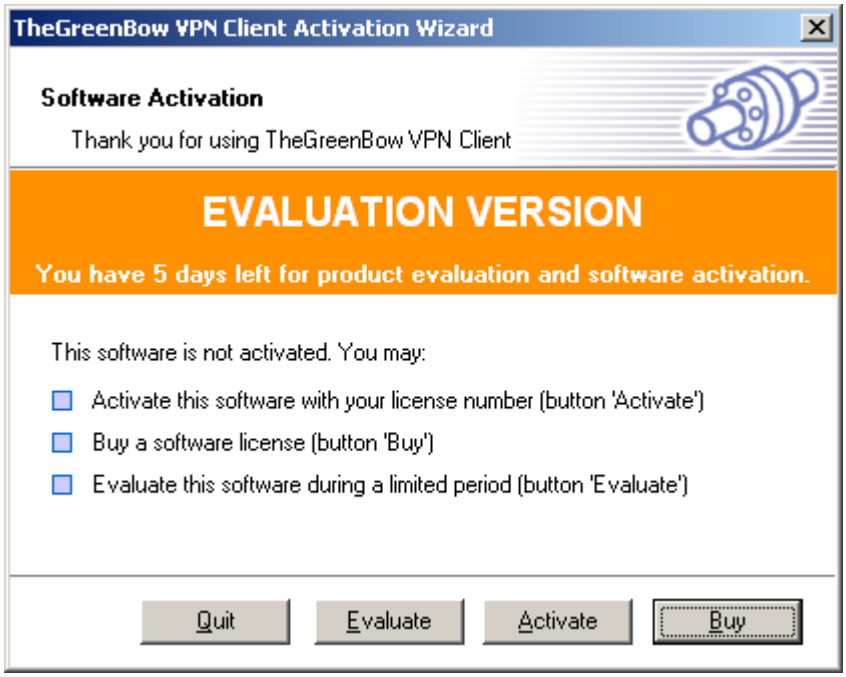
Installing TheGreenBow IPSec VPN Client

2 Installing TheGreenBow IPSec VPN Client

2.1 Software Installation

TheGreenBow VPN Client installation is a classical Windows installation that does not require specific information. After completing the installation, you will be asked to reboot your computer. After reboot and session login, a window appears with several options:

- "Quit' will close this window and software.
- "Evaluate' allows you to continue software evaluation. Evaluation period left is displayed into the orange bar above.
- "Activate' allows you to activate the software online. This requires a License Number. When clicking on 'Activate' button, an Activation Wizard pops up.
- "Buy' allows you to go online and purchase a Software License in TheGreenBow online shop.


TheGreenBow VPN Client Activation Wizard
Software Activation
Thank you for using TheGreenBow VPN Client
EVALUATION VERSION
You have 5 days left for product evaluation and software activation.
This software is not activated. You may:
Activate this software with your license number (button 'Activate')
Buy a software license (button 'Buy')
Evaluate this software during a limited period (button 'Evaluate')
Quit
Evaluate
Activate
Buy

Caution: On Windows NT, 2000 and XP, you must have administrator rights. If it is not the case, the installation stops after the language choice with an error message.

Shortcuts: After software installation, TheGreenBow VPN window can be launched:

- from user desktop, by double-clicking on TheGreenBow VPN shortcut
- from VPN Client icon available in the taskbar
- from menu Start > Programs > TheGreenBow > TheGreenBow VPN > TheGreenBow VPN Client

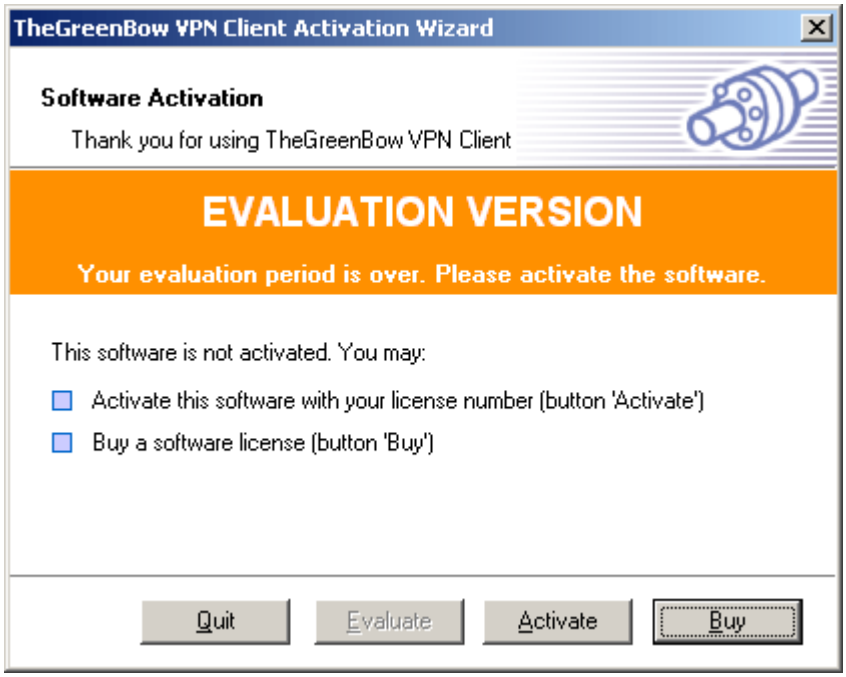
Note: Software Installation can be customized with several parameter options in command line. Please refer to the "Deployment Guide" document available on our website.

2.2 Software Evaluation

It is possible to use TheGreenBow IPSec VPN Client during the evaluation period (i.e. limited to 30 days) by clicking on 'Evaluate' button. When the IPSec VPN Client is on "Evaluation" mode, the register window appears at each start of the IPSec VPN Client. Evaluation period is displayed into

the orange bar above.

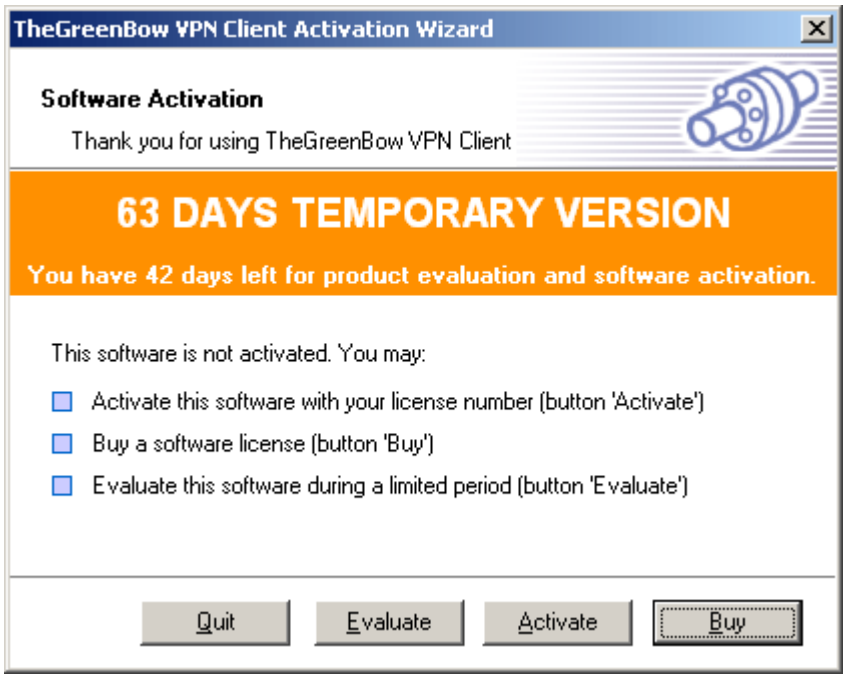
Once evaluation period expires, 'Evaluation' button is no longer available and the software is disabled.


TheGreenBow VPN Client Activation Wizard
Software Activation
Thank you for using TheGreenBow VPN Client
EVALUATION VERSION
Your evaluation period is over. Please activate the software.
This software is not activated. You may:
Activate this software with your license number (button 'Activate')
Buy a software license (button 'Buy')
Quit
Evaluate
Activate
Buy

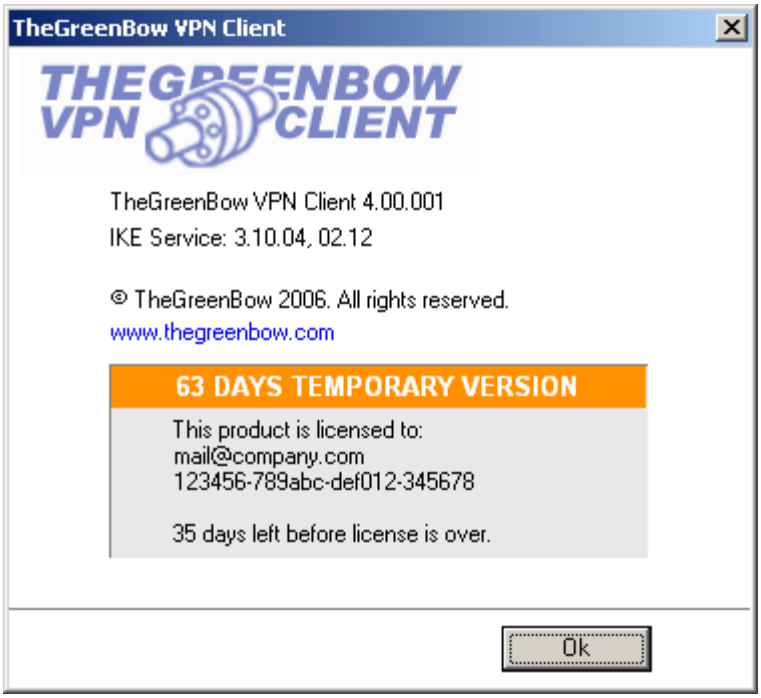
2.3 Temporary Software License

A Temporary Software License Number may be provided, for test purpose. The period of validity is between 1 and 35 weeks. To receive a Temporary Software License Number, you can contact our sales team: sales@thegreenbow.com.

The validity period of the Temporary Software License Number and the remaining time of use are shown in the first popup window of the IPSec VPN Client.
At the end of the validity period, the software cannot be run.


TheGreenBow VPN Client Activation Wizard
Software Activation
Thank you for using TheGreenBow VPN Client
63 DAYS TEMPORARY VERSION
You have 42 days left for product evaluation and software activation.
This software is not activated. You may:
Activate this software with your license number (button 'Activate')
Buy a software license (button 'Buy')
Evaluate this software during a limited period (button 'Evaluate')
Quit
Evaluate
Activate
Buy

During all the time a Temporary Software License Number is used, the activation window is available from the Configuration Panel. It enables the user to activate a new license, for example a life time License Number instead of a temporary one.
During that period, the remaining time is available through the 'About' menu as shown below:



When the Temporary Software License Number expires, the 'Evaluate' button is disabled. The user can Buy and Activate a life time software license.

Property of TheGreenBow© - Sistech SA 2000-2007

2.4 Software Activation

2.4.1 Software Activation Wizard

For use beyond the evaluation period, TheGreenBow IPSec VPN Client software must be activated. The Software Activation is a two step process which requires a License Number and an email address.

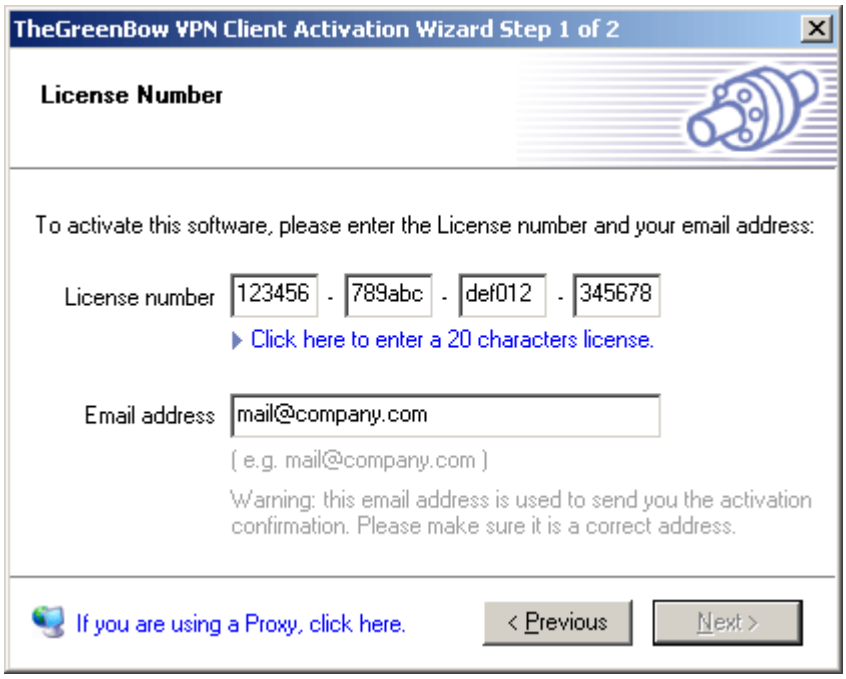
The 'Activation Wizard' can be launched from the VPN Client software as followed:

- Click on the 'Activate' button in the startup windows when you start the VPN Client.
- Click on the '?' menu and then click on "Activation Wizard...".

2.4.2 Step 1 of 2: Enter License Number

Software Activation requires a License Number.

Enter your License Number, your email address and click 'Next' as shown below:


TheGreenBow VPN Client Activation Wizard Step 1 of 2
License Number
To activate this software, please enter the License number and your email address:
License number
123456
789abc
def012
345678
Click here to enter a 20 characters license.
Email address
mail@company.com
(e.g. mail@company.com)
Warning: this email address is used to send you the activation confirmation. Please make sure it is a correct address.
If you are using a Proxy, click here.
< Previous
Next >

> Warning: if you have a 20 character License Number, switch to the 20 character "License Number" field by clicking on the link "Click here to enter a 20 character License".

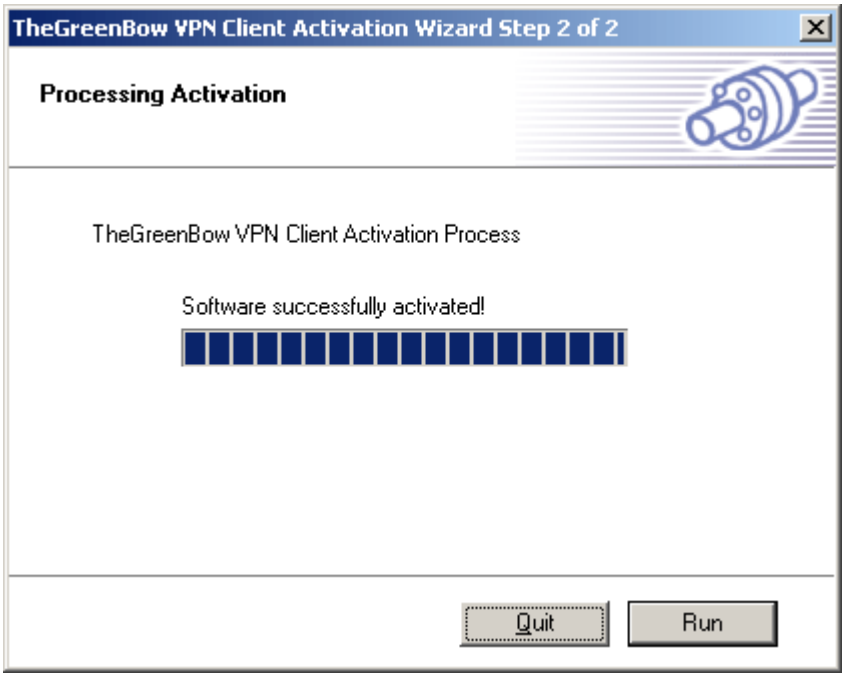
Note: Be careful the email address is correct, it will be used to send you back the activation confirmation.

Note: The email address may not be required: IT Managers can force this value during the setup, then it will not be displayed by the Software Activation Wizard. This feature can be used to centralize all the Software Activation confirmation emails to a single email address.

2.4.3 Step 2 of 2: Online Activation

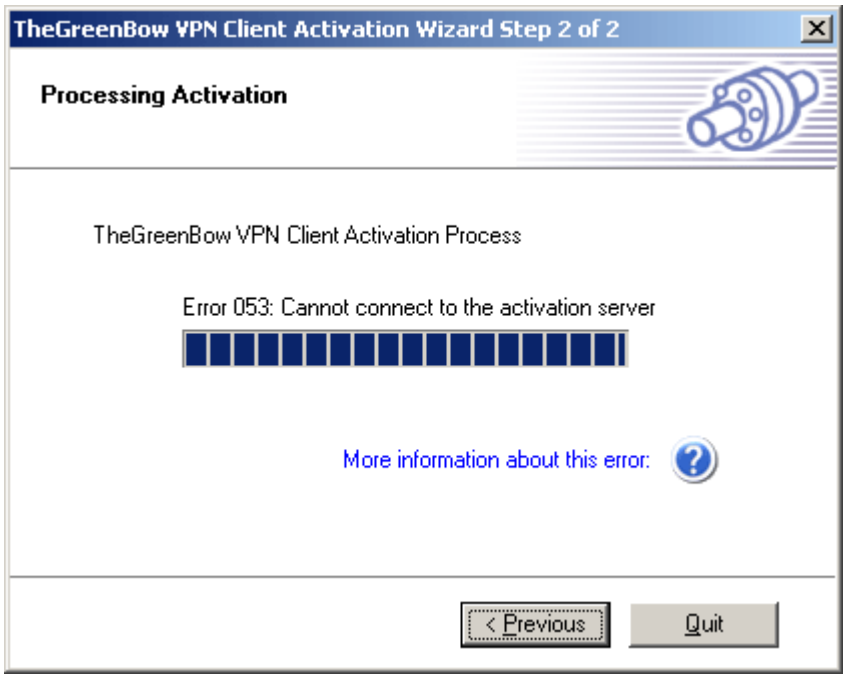
The 'Activation Wizard' will automatically connect to the online software activation server to activate the VPN Client Software. You can go back at anytime to change the License Number.

The 'Activation Wizard' will end with a successful Activation.



2.4.4 Activation Troubleshooting

Errors may occurred during the activation process. Each activation error is briefly explained on the step 2 activation window. The link "More information about this error" below the progress bar provides online full explanations and recommendations on how to proceed next.


TheGreenBow VPN Client Activation Wizard Step 2 of 2
Processing Activation
TheGreenBow VPN Client Activation Process
Error 053: Cannot connect to the activation server
More information about this error:
< Previous
Quit

Most of errors encountered may be fixed by carefully checking the following points:

1. Check you entered the correct License Number (error 031).
2. The communication with our activation server may be filtered by a proxy (error 053 or error 054). You should configure the proxy in the step 1 of the Software Activation Wizard by clicking the link at the bottom of the window.
3. The communication with our activation server may be filtered by a firewall (error 053 or error 054). Check if a personal firewall or a corporate firewall is filtering communications.
4. Our activation server may be temporarily unreachable. Try to activate the software a few minutes later.
5. Your License Number is already activated (error 033). Contact our sales team: sales@thegreenbow.com.

All activation errors are detailed online on our website:
http://www.thegreenbow.com/help.html?subject=osa&id=001

Note: If you didn't succeed to activate the software despite the previous recommendations, it is always possible to manually activate the software on our website: http://www.thegreenbow.com/activation/osa_manual.html. This enables users to immediately fully activate the software.

2.5 Software Upgrade

Warning: The VPN Client software needs to be activated once software upgrade is done. Depending on your maintenance contract, a software upgrade activation might be rejected. Please read carefully the following recommendations and check current status of your maintenance and your software release by clicking on the menu "?" then "Check for update" on the Configuration Panel.

Property of TheGreenBow© - Sistech SA 2000-2007

The success of a software upgrade activation depends on your maintenance contract:

1. During your maintenance period (which starts from your first activation), all software upgrades are allowed.
2. Once your maintenance period is expired (or if you have no maintenance contract), only minor software upgrades are allowed. Minor software upgrades are identified by the last digit of a version.

Example: My maintenance period is expired and my current software Release is 3.12. I only can upgrade to Release 3.13 till 3.19. I cannot upgrade to Release 3.20, 3.30 or 4.00.

If you want to subscribe or extend your maintenance period, please contact our sales team: sales@thegreenbow.com

Note: The VPN Configuration is saved during a Software Upgrade and automatically enabled again within the new release.

2.6 Software Uninstallation

TheGreenBow IPSec VPN Client can be uninstalled:

- from Windows Control Panel by selecting 'Add/Remove programs'
- from Start Menu > Programs > TheGreenBow > VPN > 'Uninstall IPSec VPN Client'

Part III

Quick HowTo's

3 Quick HowTo's

3.1 HowTo Open VPN tunnel?

How to open a tunnel (once VPN configuration is set):
- Connection panel > Open
- SystemTray > click on 'Open xxx'
- 'Automatic as soon as traffic' is detected
- 'Automatic as soon as USB stick is inserted'
- 'Automatic as soon as MS Windows starts' (before or after logon)
- Double click on a VPN Configuration (e.g. icon on desktop, email attachment)

3.2 HowTo Troubleshoot VPN tunnel?

How to troubleshoot a VPN tunnel?

You will be able to find all troubleshooting issues, listed in the following documents on our website:
- TroubleShooting Document (pdf).
- Online help (html).
- Online Software Activation (html).
- Use the Default VPN Configuration to test you network.
- IPSec VPN Client FAQs.

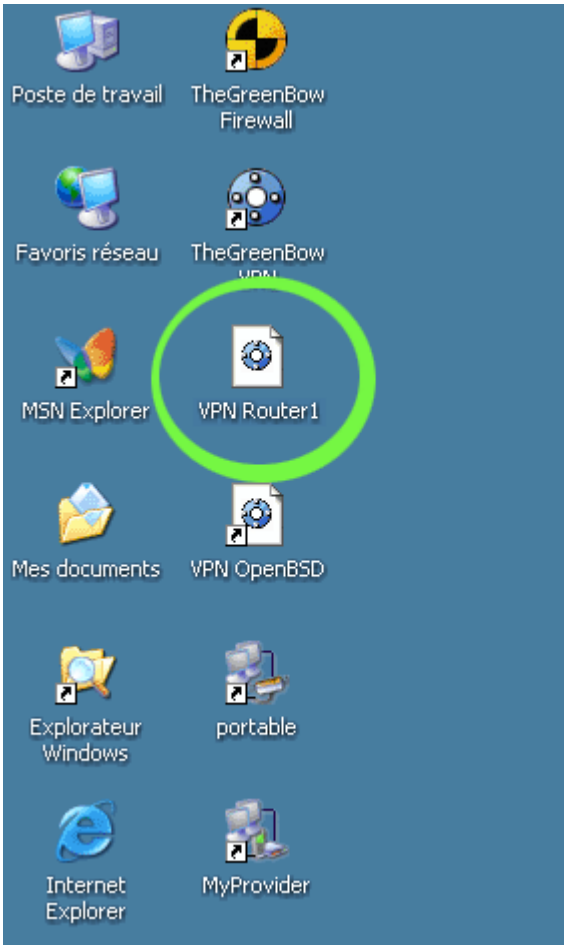
3.3 HowTo import with double click on VPN Configuration icon?

Also known as 'Dial up mode': A tunnel may be opened via a double-click on a VPN Configuration (i.e. extension '.tgb' file). This feature enables to create various VPN Configuration on the windows desktop, and to open tunnels by clicking on these VPN Configuration shortcut icon.

To create a VPN Configuration shortcut icon on the desktop:
Step 1: Configure the tunnel in 'Configuration Panel'
Step 2: In 'Phase2 Advanced Settings', configure the tunnel to 'Automatically open this tunnel when the VPN Client starts'
Step 3: Export the VPN Configuration onto your computer desktop.

Note : You may protect the VPN Configuration with a password as it is exported. This password will be asked each time the tunnel is clicked on.

Property of TheGreenBow© - Sistech SA 2000-2007



Property of TheGreenBow© - Sistech SA 2000-2007

Part IV

Navigating the User Interface

4 Navigating the User Interface

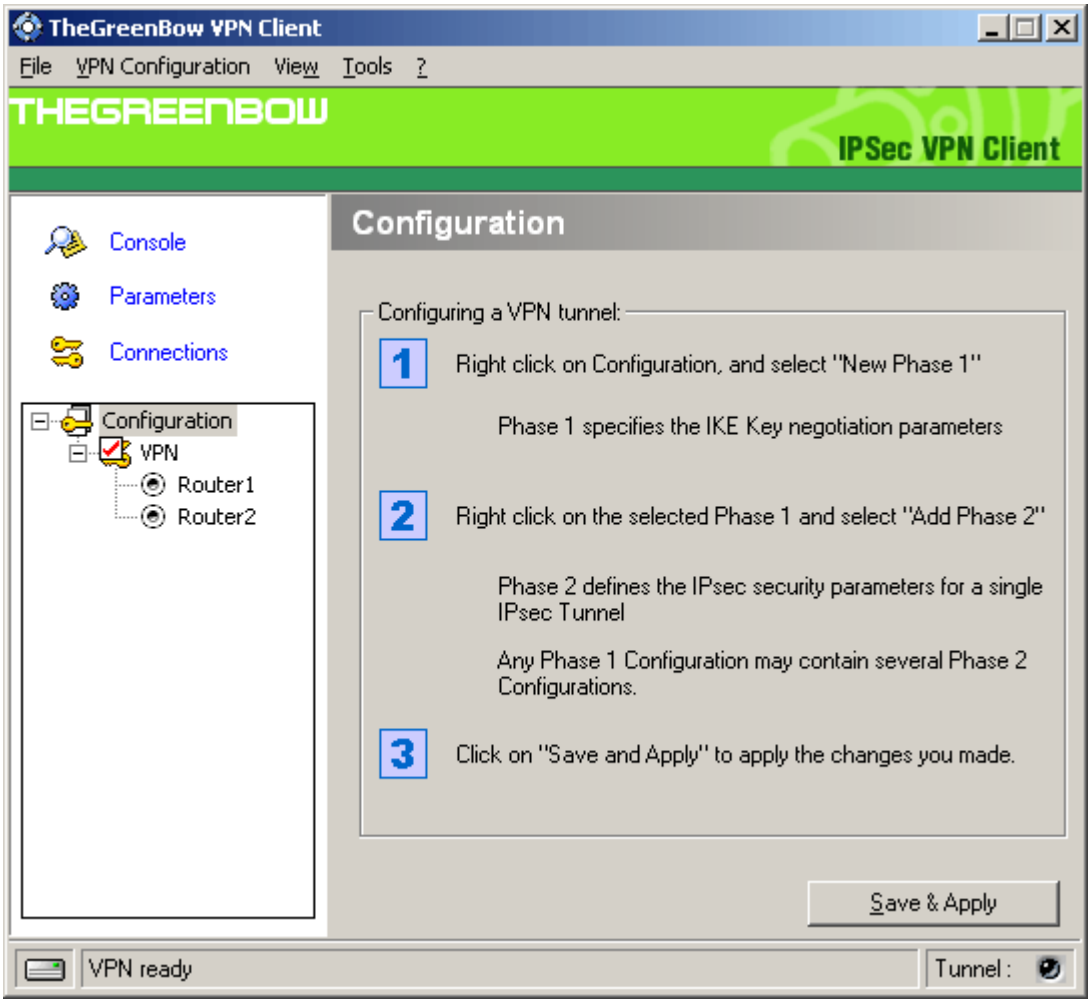
4.1 User interface elements

TheGreenBow IPSec VPN Client is fully autonomous and can start and stop tunnels without user intervention, depending on traffic to certain destinations. However it requires a VPN configuration.

The IPSec VPN Client configuration is defined in a VPN configuration file. The software user interface allows creating, modifying, saving, exporting or importing the VPN configurations together with security elements (e.g. Preshared key, Certificates, ...).

The user interface is made of several elements:

- Configuration Panel
- Connection Panel
- Main menus
- System Tray Icon
- Status bar
- Wizards
- Preferences



Property of TheGreenBow© - Sistech SA 2000-2007

4.2 System Tray Icon

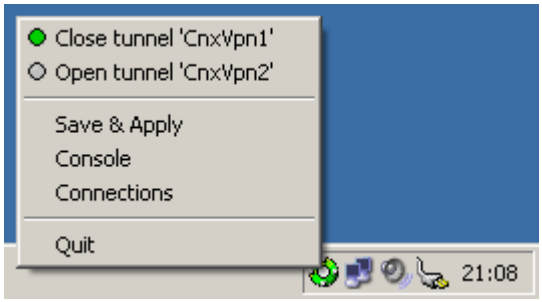
The VPN Client user interface can be launched via a double click on application icon (Desktop or Windows Start menu) or by single click on application icon in system tray. Once launched, the VPN Client software shows an icon in the system tray that indicates whether a tunnel is opened or not, using color code.

VPN Client application color code is the following

Blue icon: no VPN tunnel is opened

Green icon: at least one VPN tunnel is opened

A left-button click on VPN icon opens configuration user interface.



A right-button click shows the following menu:

- "Quit' will close established VPN tunnels, stops the configuration user interface.
- "Save & Apply' will close established VPN tunnels, apply latest VPN configuration modification and reopen all the VPN tunnels.
- "Console' shows log window.
- "Connections' opens the list of already established VPN tunnels. You can configure tunnels to open up automatically when the software starts.
- List of configured tunnels with current status. Tunnels can be opened or closed from this menu as well.

Tooltips over VPN Client icon shows the connection status of the VPN tunnel:

- "Tunnel <tunnelname>' when one or more tunnels are established
- "Wait VPN ready...' when the IKE service is reinitializing
- "TheGreenBow VPN Client' when the VPN Client is up but with no opened tunnel.

4.3 Keyboard Shortcuts

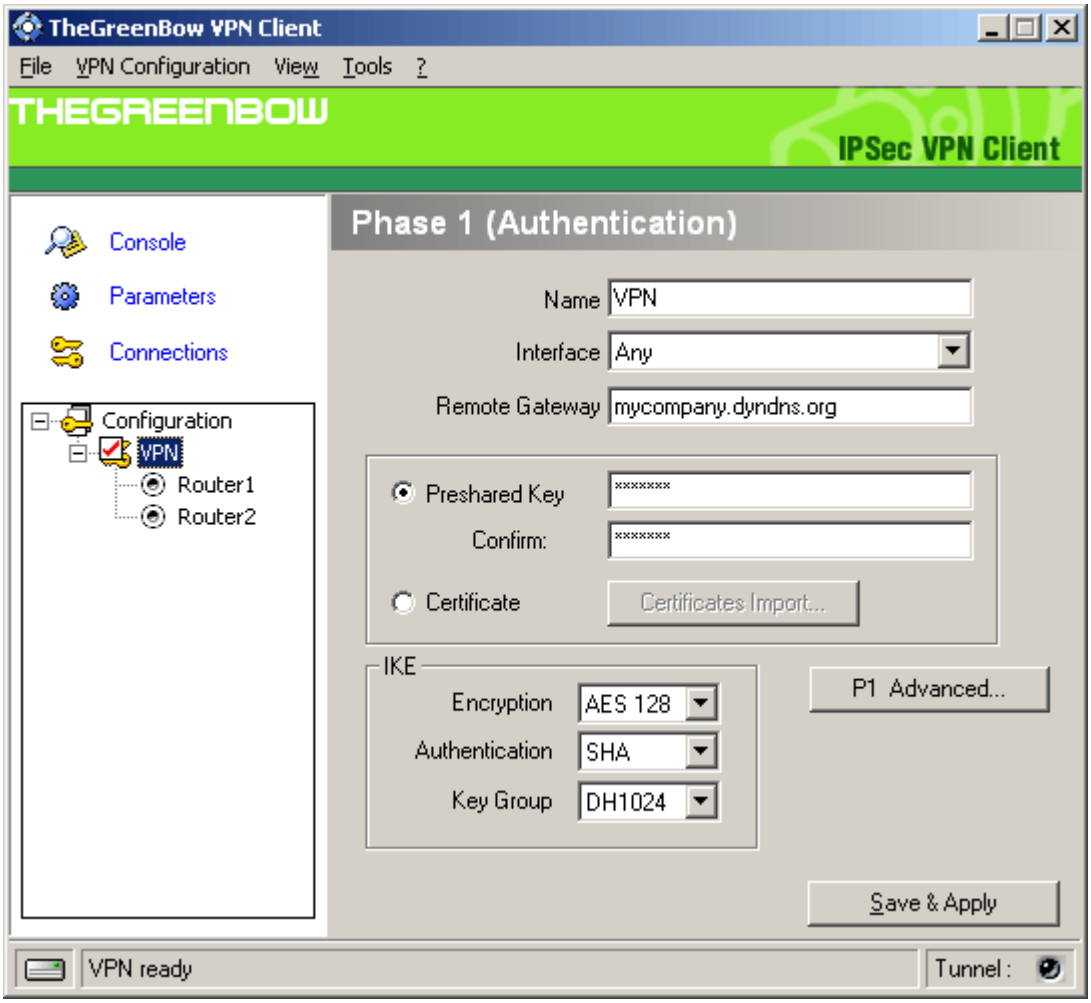
This feature improves the usual manipulations.

Shortcut	Action
Ctrl + P	Switches between the Configuration Panel and the Connection Panel. Note: in case, the Configuration Panel is protected with a password, the user will be asked for this password when he tries to switch to the Configuration Panel.
Ctrl + C	Opens the VPN Console.
Ctrl + A	'Save & Apply' a VPN Configuration.

4.4 Configuration Panel

The Configuration Panel is made of several elements:

- Three buttons 'Console', 'Parameters' et 'Connections' (left column)
- A tree list window (left column) that contains all the IKE and IPSec configurations
- A configuration window (right column) that shows the associated tree level.



A VPN Configuration file (i.e. extension '.tgb') can be drag and dropped onto the Configuration Panel. This feature enables to easily apply a new VPN configuration. If a tunnel is configured to be 'opened when the VPN Client starts' (see section 'Phase2 Advanced Settings'), it will be immediately opened as soon as the new VPN Configuration is applied ('Save & Apply').

4.4.1 Main Menus

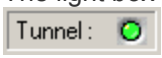
There are several menus as followed:

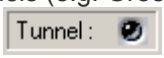
- 'File' menu is used to Import or Export a configuration. It is also used to choose the location of the VPN Configuration: local, USB, server, Token. It is finally used to configure miscellaneous preferences such as the way the VPN Client may start (e.g. before or after logon, ...).
- 'VPN Configuration' menu contains all actions from tree control right-click menu. 'Configuration' menu gives also access to the 'Configuration Wizard'.
- 'View' menu contains the 'Configuration' of what the user can have access to.
- 'Tools' menu contains 'Console' and 'Connections' choice.

- '?' menu gives access to 'check for update', 'online help' and window 'About'. '?' menu also gives access to the 'Activation Wizard'.

4.4.2 Status Bar

The status bar displays several information:

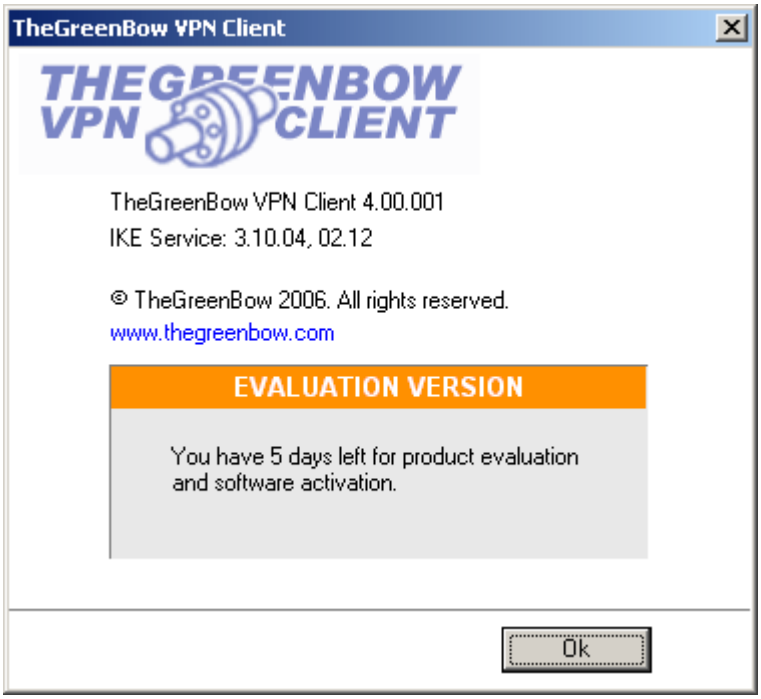
- The left side box indicates the VPN configuration location. For example, if the "USB Mode" is set, the image will show a USB stick, enabled or not depending on the presence of a valid VPN USB stick.
- The central box gives some information about VPN Client Software status (e.g. "opening tunnel in progress", "saving configuration rules in progress", "VPN Client start up in progress", …)
- The light box (right side) gives some information about tunnels (e.g. Green light 

means at least one tunnel is open, Gray light 

means no tunnel open)

4.4.3 Windows "About"

The 'About' window provides the VPN Client software version and software activation information. There is also an URL to our web site.

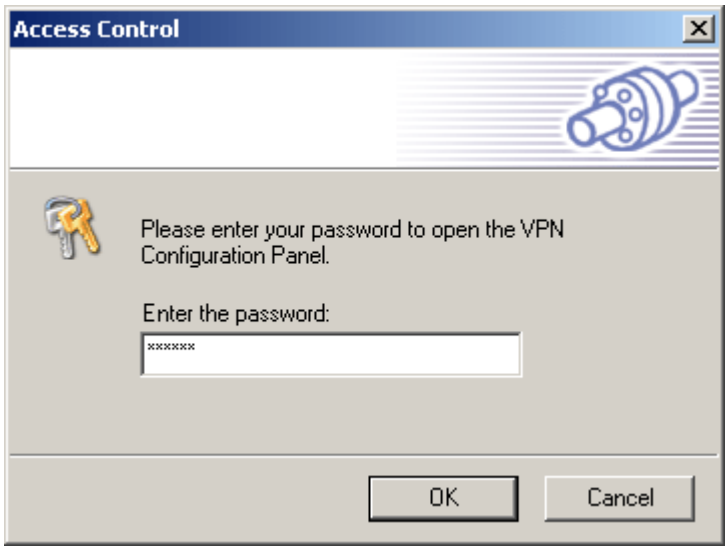


4.4.4 Access Control & Hidden Interface

This feature is especially designed for IT Managers. It enables to lock the access to the Configuration Panel, and to restrict with password the use of the IPSec VPN Client to the 'Connection Panel' and/or to the systray menu. Therefore, users cannot modify the VPN Configuration anymore, and misconfiguration are avoided.

Once configured, the user will be asked for the password:

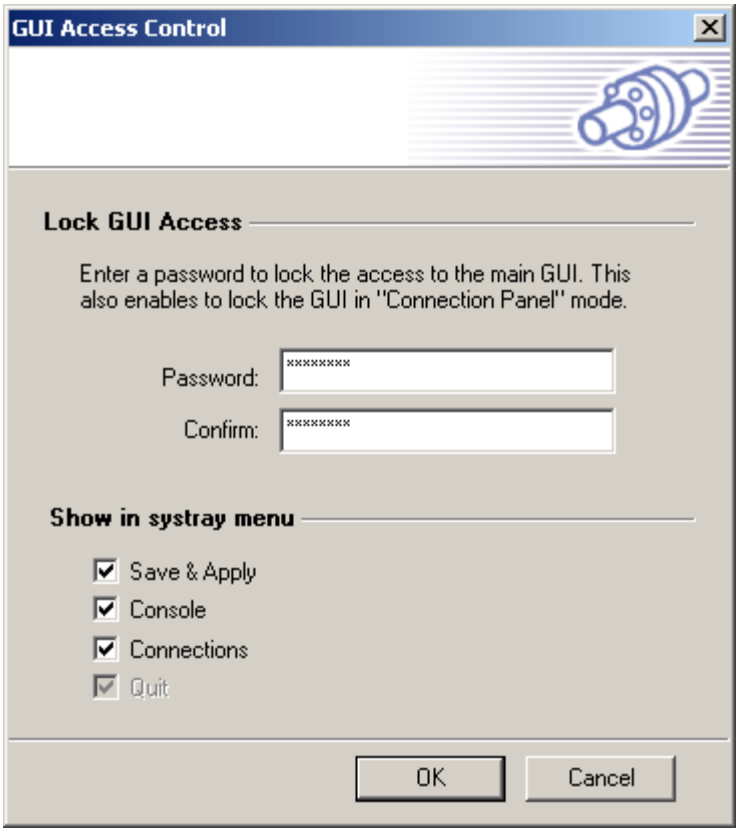
1. when he clicks (or double-clicks) on the systray IPSec VPN Client icon
2. when he switches from the "Connection Panel" to the "Configuration Panel".



This password may be configured as an option of the setup (see section 'Setup options').

The Access Control Window available through the menu 'View > Configuration' in the Configuration Panel, also enables to configure the systray menu items. Thus, the IT Manager can restrict the software access, from a full access to a completely hidden interface.

Property of TheGreenBow© - Sistech SA 2000-2007

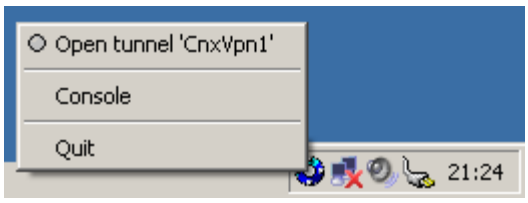


To remove the access control, just empty both fields 'Password' and 'Confirm' then click 'OK'.

Note: The 'Quit' item for the systray menu is disabled in the standard version of the software. It can nevertheless be removed during the software setup, through the setup option "`-menuitem`" (see section 'Setup option')

The access control with a password only concerns the 'Configuration Panel'. The access to the 'Connection Panel' is never controlled by password.

In case Access Control has been set, the 'Configuration Panel' can not be opened and showed by double-clicking on desktop icon, by selecting Start menu. Right-click over the icon in taskbar is limited to "Console" access, quitting the software, and opening/closing the configured tunnels:



4.4.5 Wizards

There are two Wizards available:

- VPN Configuration Wizard can be launched from Menu 'VPN Configuration' > 'Config Wizard'.
- Software Activation Wizard can be launched from Menu '?' > 'Activation Wizard'.

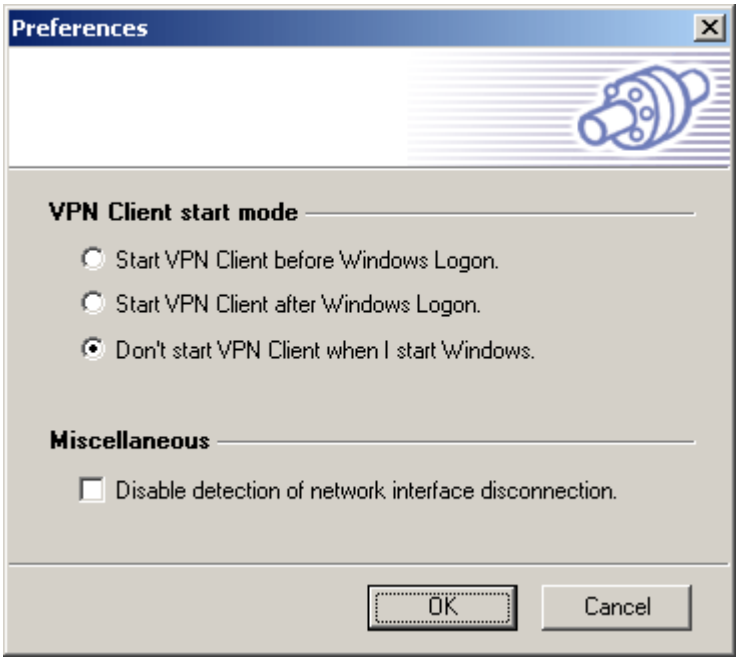
Property of TheGreenBow© - Sistech SA 2000-2007

4.4.6 Preferences

'Preferences' window allows you to define:

- Start up mode of the software. Those modes can be configured in the software setup (see section 'Setup options').
- Enable/Disable the detection of interface disconnection feature

Preferences are available via Menu 'File' and click 'Preferences'.



VPN Client start mode
TheGreenBow IPSec VPN Client software has several start up mode, such as:

- Start IPSec VPN Client software before MS Windows logon: this mode can be used for secure remote login
- Start IPSec VPN Client software after MS Windows logon
- Don't start IPSec VPN Client when I start MS Windows: IPSec VPN Client is launched by user or from a script ("manual" mode)

Miscellaneous
Disable detection of interface disconnection allows the IPSec VPN Client maintain tunnels opened while the network interface disconnects momentarely but very often. This type of behavior occurs when the interface used to open tunnels is unstable such as WiFi, GPRS and all 3G interfaces.

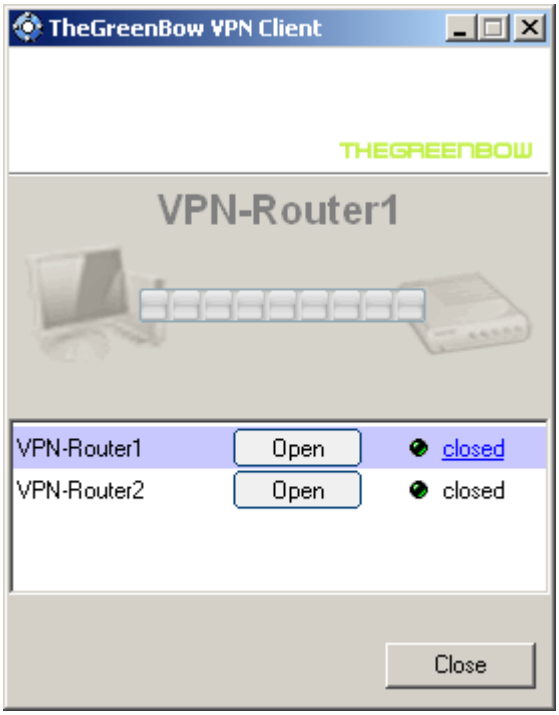
4.5 Connection Panel

The Connection Panel enables users to open, close and get clear information about every tunnel that have been configured. This is all the end-user needs to open and close tunnels.
This feature clearly help both IT Managers (who configure the VPN connections) and users (who only open or close VPN connections) with their own usage.

The Connection Panel is made of several elements:

- An animated network diagram showing information on current tunnel (top)
- A list of all configured tunnels with 'open/close' button (below diagram)

It's always possible to switch from the Connection Panel to the Configuration Panel through the system menu (menu 'Configuration Panel') or via the shortcut 'Ctrl + P' (see section 'Shortcuts').



Property of TheGreenBow© - Sistech SA 2000-2007

Part V

Connection Panel

5 Connection Panel

5.1 Connection Panel basics

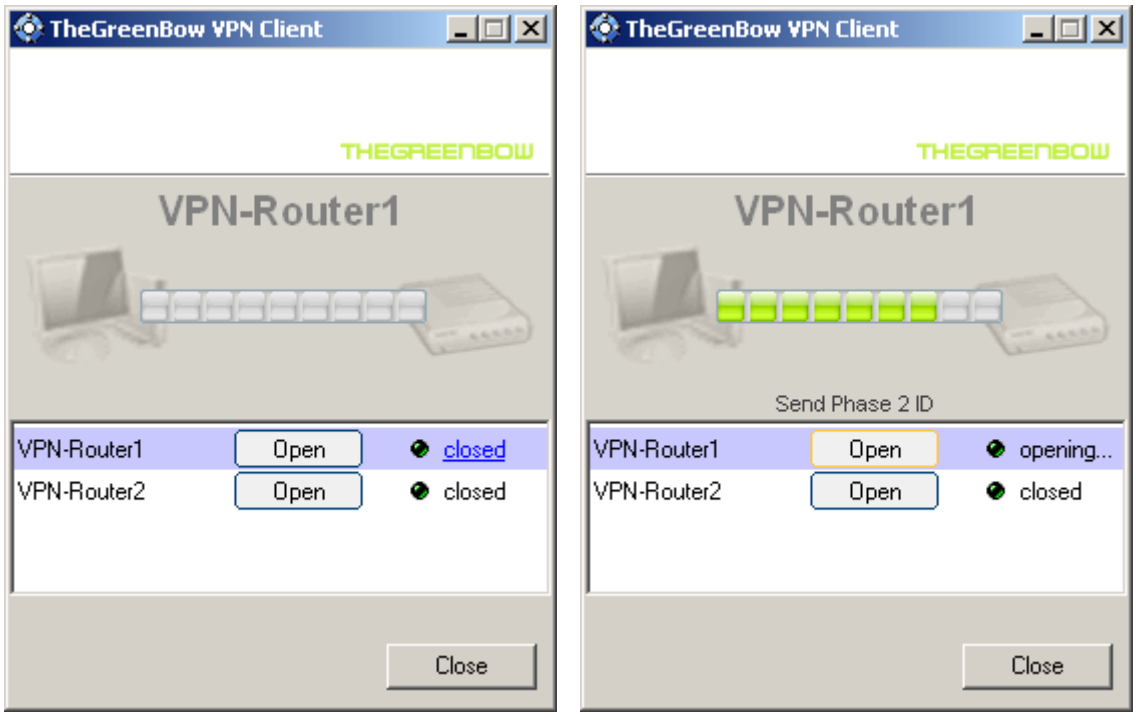
The Connection Panel enables users to open, close and get clear information about every tunnel that have been configured. This is all the end-user needs to open and close tunnels.

The Connection Panel is made of several elements:

- An animated network diagram showing information on current tunnel (top)
- A list of all configured tunnels with 'open/close' button (below diagram)

The user simply clicks on the 'Open' button of a tunnel to open this tunnel. The 'Open' button automatically switch to 'Close' when then tunnel is opened. One click on the name of the tunnel automatically opens the Configuration Panel, enabling to change the tunnel configuration. This feature is disabled when the Connection Panel is protected with a password (see section 'Access Control').

It's always possible to switch from the Connection Panel to the Configuration Panel through the system menu (menu 'Configuration Panel') or via the shortcut 'Ctrl + P' (see section 'Shortcuts').

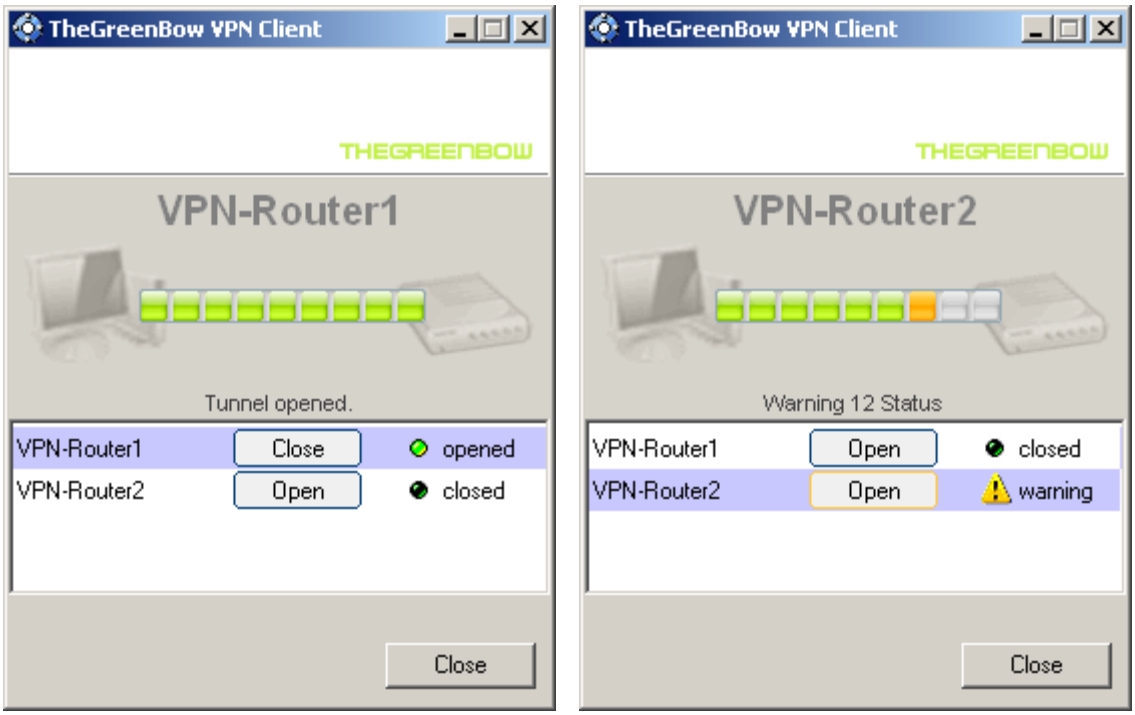


It is also possible to automatically apply a new VPN Configuration by a drag & drop of a VPN Configuration onto the Connection Panel. If a tunnel is configured to be automatically opened when VPN Client starts (see section 'Phase2 Advanced Settings'), it will be immediately opened as soon as the new VPN Configuration is applied ('Save & Apply').

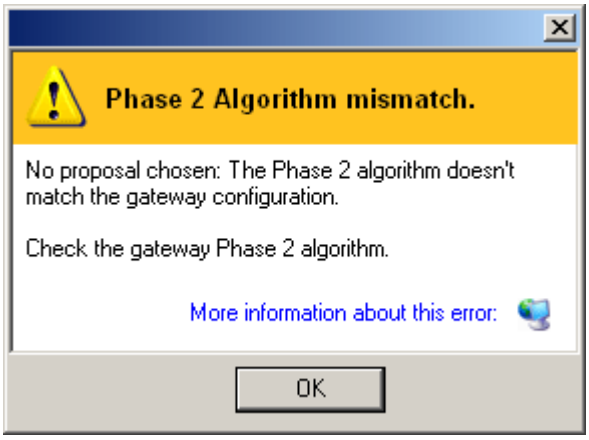
Property of TheGreenBow© - Sistech SA 2000-2007

5.2 More info about Connections

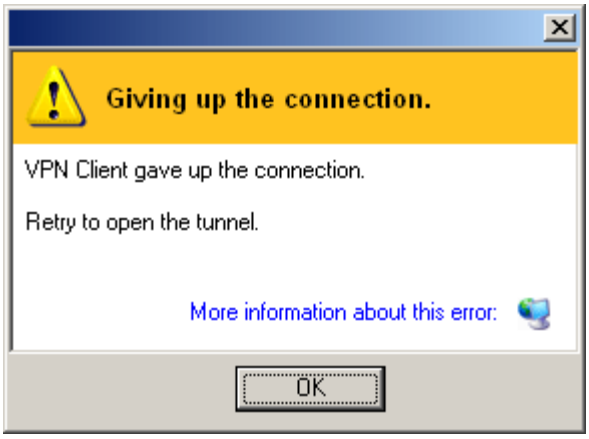
If problems occur during the tunnel opening process, a warning is shown on the right of the tunnel list.



A link associated to the warning automatically opens the 'Warning' tab control and shows a detailed message about the problem. Explicit warning messages help users and IT Managers to find the VPN issue. These popups are also linked ("more information" link) to our online help web pages that detail symptoms and give clues for troubleshooting.


Phase 2 Algorithm mismatch.
No proposal chosen: The Phase 2 algorithm doesn't match the gateway configuration.
Check the gateway Phase 2 algorithm.
More information about this error:
OK

Property of TheGreenBow© - Sistech SA 2000-2007


Giving up the connection.
VPN Client gave up the connection.
Retry to open the tunnel.
More information about this error:
OK

Property of TheGreenBow© - Sistech SA 2000-2007

Part VI

VPN Configuration

6 VPN Configuration

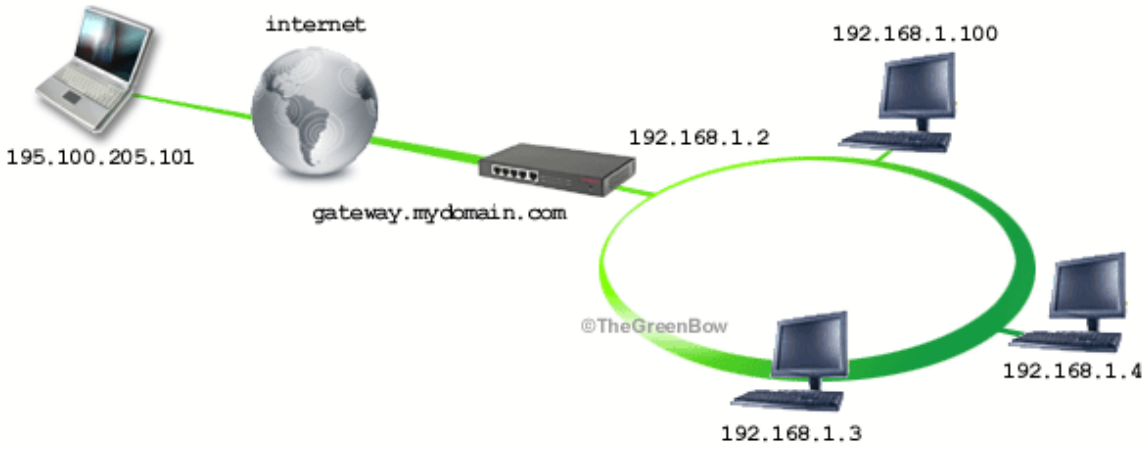
6.1 Configuration Wizard

6.1.1 Three step Configuration Wizard

TheGreenBow IPSec VPN Client provides a Configuration Wizard that allows the creation of VPN configuration in three easy steps. This Configuration Wizard is designed for remote computers that need to get connected to a corporate LAN through a VPN gateway. Remember that Peer to Peer mode is also available.

Let take the following example:

- The remote computer has a dynamically provided public IP address.
- It tries to connect the Corporate LAN behind a VPN gateway that has a DNS address "gateway.mydomain.com".
- The Corporate LAN address is 192.168.1.xxx. e.g. the remote computer want to reach a server with the IP address: 192.168.1.100.

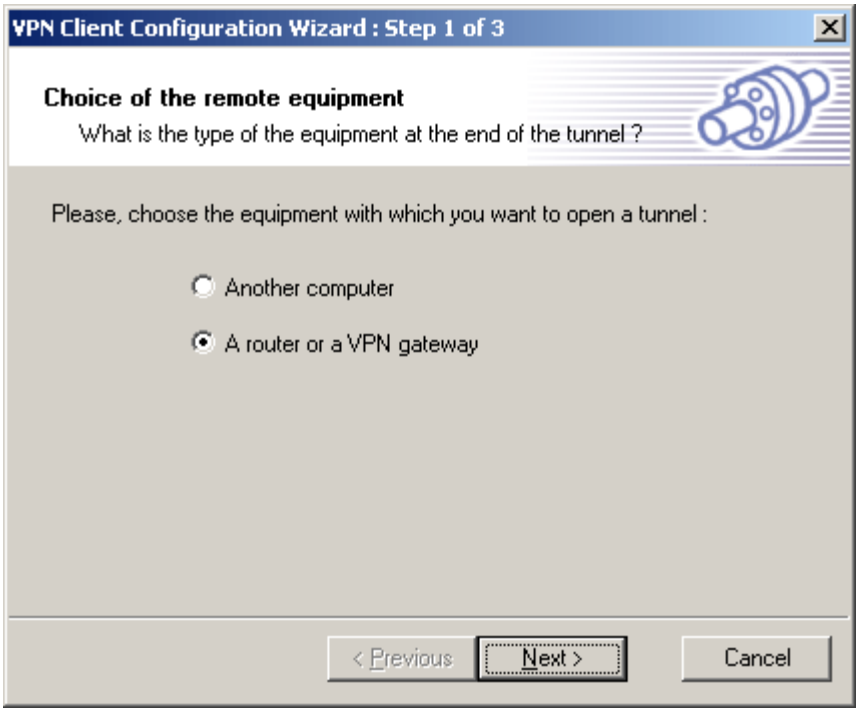


For configuring this connection, open wizard's window by selecting menu "Configuration > Wizard"

6.1.2 Step 1 of 3: Choice of remote equipment

You must specify the type of the equipment at the end of the tunnel: VPN gateway.

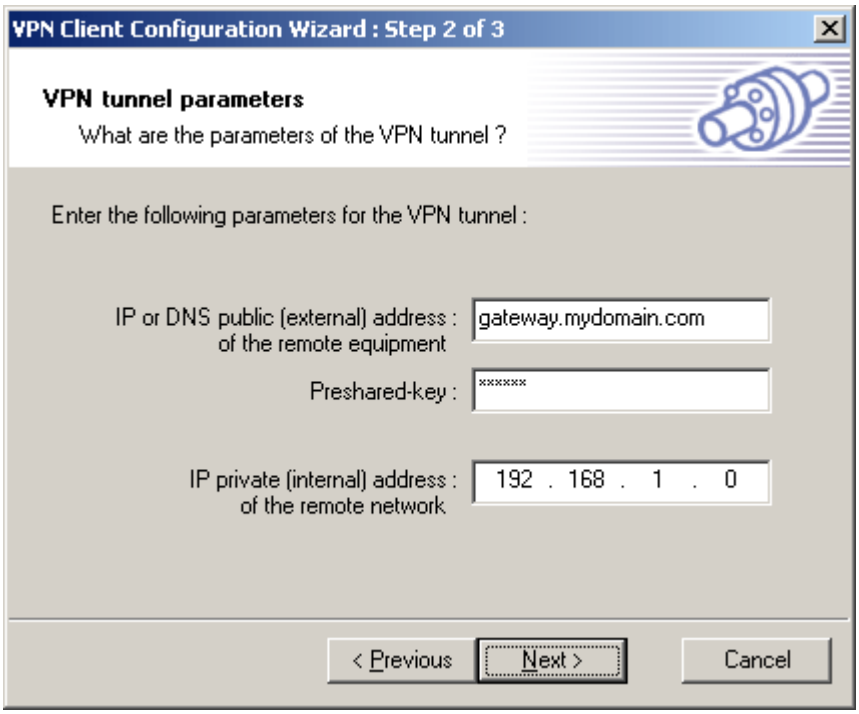
Property of TheGreenBow© - Sistech SA 2000-2007


VPN Client Configuration Wizard : Step 1 of 3
Choice of the remote equipment
What is the type of the equipment at the end of the tunnel ?
Please, choose the equipment with which you want to open a tunnel :
Another computer
A router or a VPN gateway
< Previous
Next >
Cancel

6.1.3 Step 2 of 3: VPN tunnel parameters

You must specify the following information:

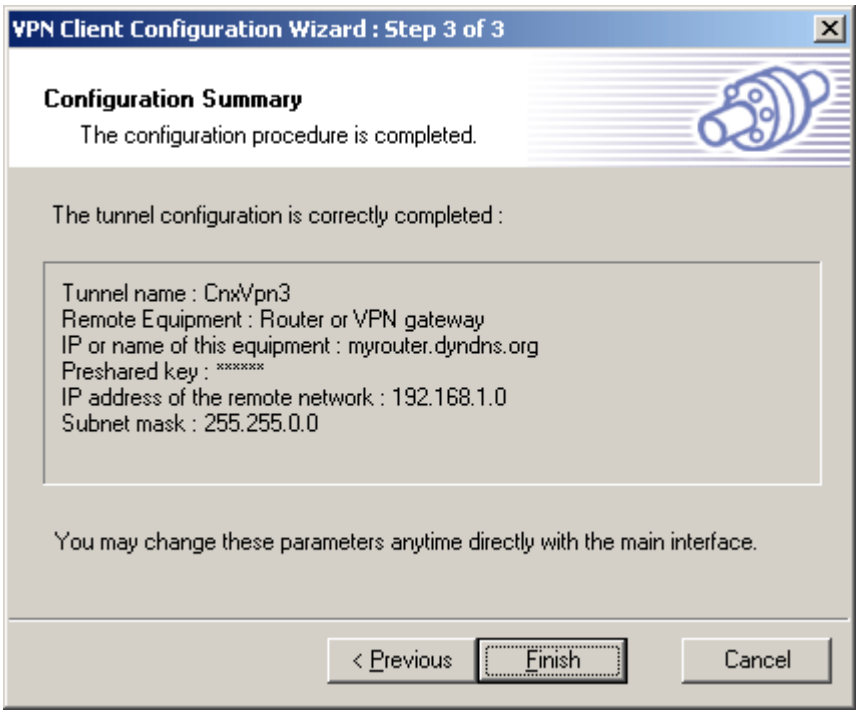
- the public (network side) address of the remote gateway
- the preshared key you will use for this tunnel (this preshared key must be the same in the gateway)
- the IP address of your company LAN (e.g. specify 192.168.1.0)


VPN Client Configuration Wizard : Step 2 of 3
VPN tunnel parameters
What are the parameters of the VPN tunnel ?
Enter the following parameters for the VPN tunnel :
IP or DNS public (external) address : of the remote equipment
gateway.mydomain.com
Preshared-key :
******
IP private (internal) address : of the remote network
192 . 168 . 1 . 0
< Previous
Next >
Cancel

Property of TheGreenBow© - Sistech SA 2000-2007

6.1.4 Step 3 of 3: Summary

The third step summaries your new VPN configuration. Other parameters may be further configured directly via the 'Configuration Panel' (e.g. Certificates, virtual IP address, etc..).


VPN Client Configuration Wizard : Step 3 of 3
Configuration Summary
The configuration procedure is completed.
The tunnel configuration is correctly completed :
Tunnel name : CnxVpn3
Remote Equipment : Router or VPN gateway
IP or name of this equipment : myrouter.dyndns.org
Preshared key : ******
IP address of the remote network : 192.168.1.0
Subnet mask : 255.255.0.0
You may change these parameters anytime directly with the main interface.
< Previous
Finish
Cancel

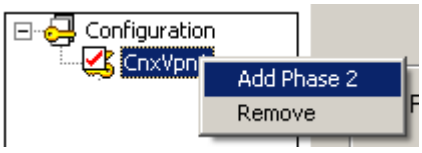
6.2 VPN Tunnel Configuration

6.2.1 How to create a VPN Tunnel ?

To create a VPN tunnel from the Configuration Panel (without using the Configuration Wizard), you must follow the following steps:

1. Right-click on 'Configuration' in the tree list window and select 'New Phase 1'

2. Configure Authentication Phase (Phase 1)
3. Right-click on the 'new Phase 1' in the tree control and select 'Add Phase 2'



4. Configure IPSec Phase (Phase 2)
5. Once the parameters are set, click on 'Save & Apply' to take into account the new configuration. That way the IKE service will run with the new parameters
6. Click on 'Open Tunnel' for establishing the IPSec VPN tunnel (only in "IPSec Configuration" window)

Please refer to Phase 1 and Phase 2 for settings descriptions.

6.2.2 Multiple Authentication or IPSec Configuration Phase

Several Authentication Phases (Phase1) can be configured. Therefore, one computer can establish IPSec VPN connections with several gateways or other computers (peer to peer).

Similarly, several IPSec Configuration (Phase 2) can be created for a same Authentication Phase (Phase 1).

6.2.3 Advanced Features

Advanced features and parameters can be defined for Phase 1 and Phase 2.

Those defined in Phase 1 apply to all Phase 2 created in current VPN Configuration:

- Enable/Disable Config-Mode
- Enable/Disable NAT-T Agressive Mode
- Enable/Disable Redundant Gateway
- Select NAT-T mode (Forced, Disabled or Automatic)
- Set X-Auth Login/password with pop up option

Those defined in Phase 2 only apply to the associated Phase 2:

- Automatic Open Mode
- Choose Script/Application to be launched when tunnel opens
- Manual settings of DNS/WINS server addresses

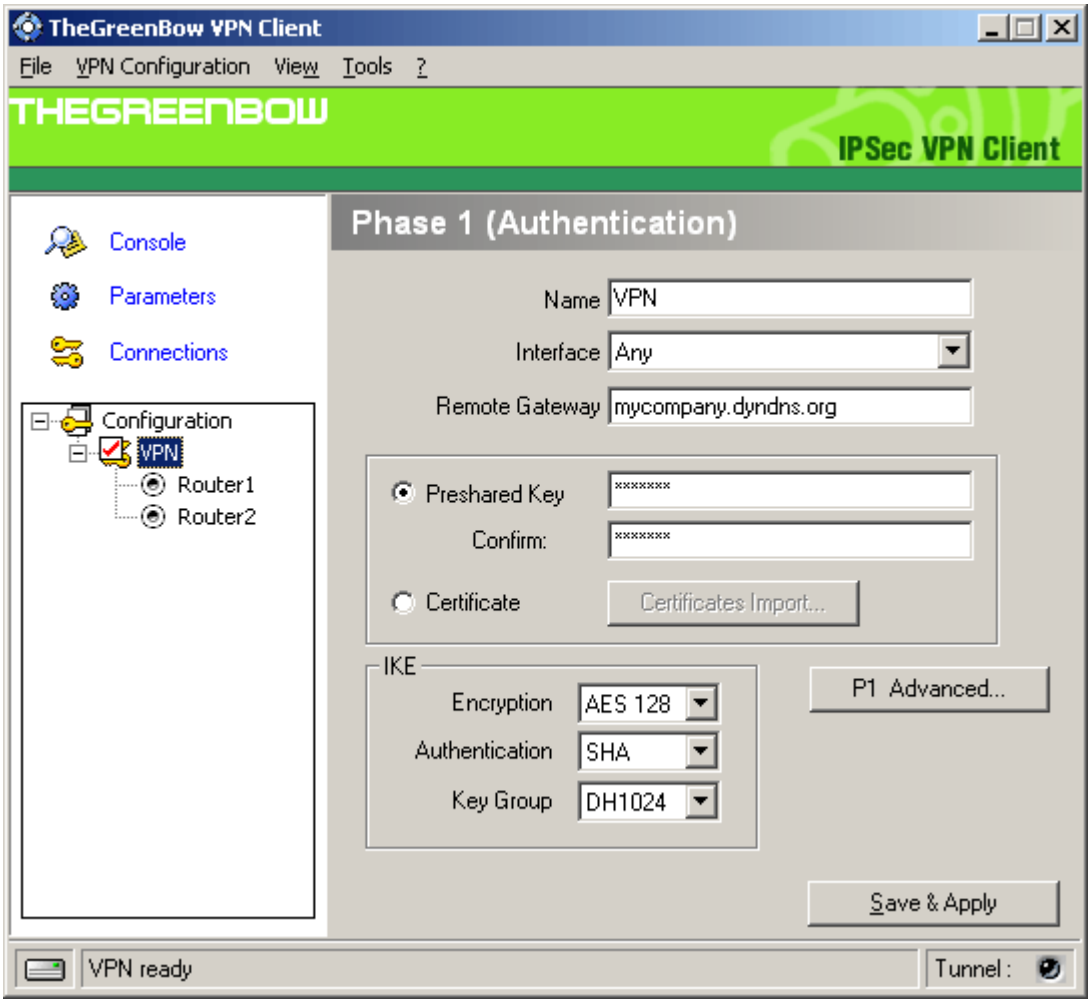
6.3 Authentication or Phase 1

6.3.1 What is Phase 1 ?

'Authentication' or 'Phase 1' window will concern settings for Authentication Phase or Phase 1. It is also called IKE Negotiation Phase.

Phase 1's purpose is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. As part of Phase 1, each end system must identify and authenticate itself to the other.

6.3.2 Phase 1 Settings Description



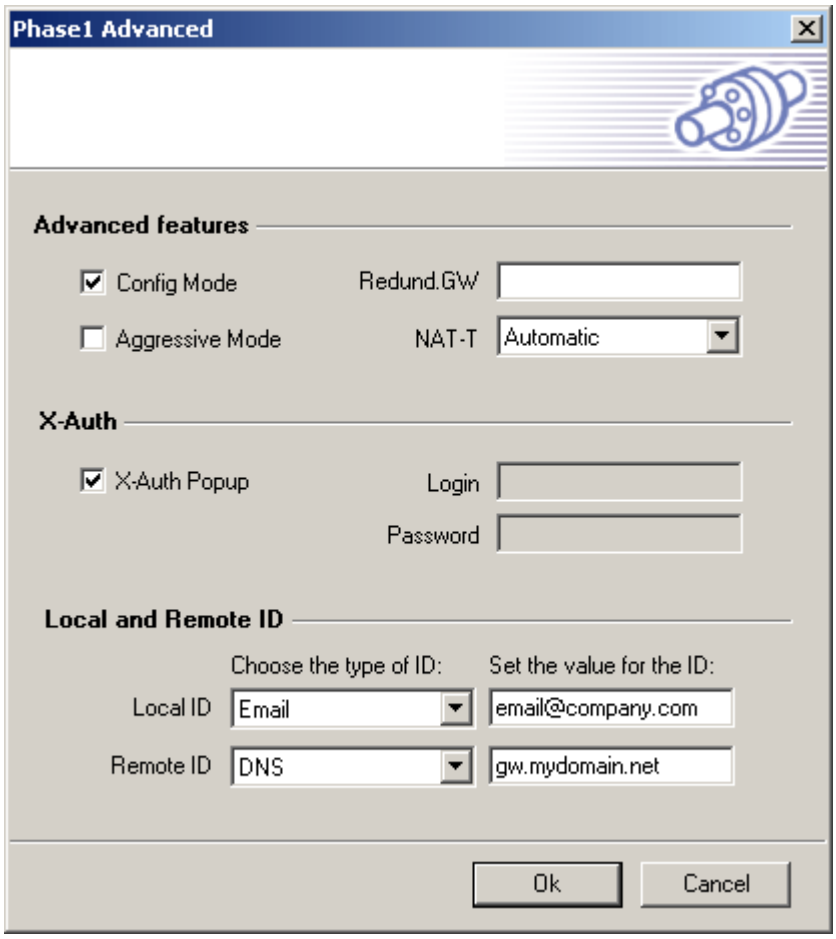
Name	Label for Authentication phase used only the configuration user interface. This value is never used during IKE negotiation. It is possible to change this name at any time and read it in the tree control. Two Phase 1 can not have the same name.
Interface	IP address of the network interface of the computer, through which VPN connection is established. If the IP address may change (when it is received dynamically by an ISP), select "Any".
Remote Gateway	IP address or DNS address of the remote gateway (in our example: gateway.mydomain.com). **This field is mandatory**.
Pre-shared key	Password or key shared with the remote gateway.
Certificate	X509 certificate used by the VPN Client . Click on 'Certificate Import..' to choose the certificate source: PEM files, PKCS#21 file or SmartCard (see section How to configure Certificates). One Certificate per tunnel can be configured.
IKE encryption	Encryption algorithm used during Authentication phase (3DES, AES, ...).
IKE authentication	Authentication algorithm used during Authentication phase (MD5, SHA, ...).
IKE key group	Diffie-Hellman key length.

For more advanced settings, click on 'P1 Advanced'.

Property of TheGreenBow© - Sistech SA 2000-2007

6.3.3 Phase1 Advanced Settings Description

For advanced features & parameters, click on 'P1 Advanced' button into Phase1 panel.



Config-Mode

If checked, the VPN Client will activate Config-Mode for this tunnel. Config-Mode allows to the VPN Client to fetch some VPN Configuration information from the VPN gateway. If Config-Mode is enabled, and provided that the remote Gateway supports Config-Mode, the following parameters will be negotiated between the VPN Client and the remote Gateway during the IKE exchange (Phase 1):

- Virtual IP address of the VPN Client
- DNS server address (optional)
- WINS server address (optional)

In case Config-Mode is not available on the remote gateway, you may refer to section 'Phase2 Advanced' settings to manually set DNS and WINS server addresses into the IPSec VPN Client.

Aggressive Mode

If checked, the VPN Client will used aggressive mode as negociation mode with the remote gateway.

Property of TheGreenBow© - Sistech SA 2000-2007

Redundant GW

This allows the VPN Client to open an IPSec tunnel with an alternate gateway in case the primary gateway is down or not responding. Enter either the IP address or the url of the Redundant Gateway (e.g. router.dyndns.com).

- TheGreenBow VPN Client will contact the primary gateway to establish a tunnel. If it fails after several tries (default is 5 tries, configurable in "Parameters" panel > "Retransmissions" field) the Redundant Gateway is used as the new tunnel endpoint. Delay between two retries is about 10 seconds.
- In case primary gateway can be reached but tunnel establishment fails (e.g. VPN configuration problems) then the VPN Client won't try to establish tunnels with the redundant gateway. Configurations need modifications.
- If a tunnel is successfully established to the primary gateway with DPD feature (i.e. Dead Peer Detection) negotiated on both sides, when the primary gateway stops responding (e.g. DPD detects non-responding remote gateways) the VPN Client immediately starts opening a new tunnel with the redundant gateway.
- The exact same behaviour will apply to the redundant gateway. This means that the VPN Client will try to open primary and redundant gateway until the user exits software or click on 'Save & Apply'.

NAT-T mode

The NAT-T mode allows Forced, Disabled and Automatic.
The NAT-T "Disabled" prevents the IPSec VPN Client and the VPN gateway to start NAT-Traversal.
The NAT-T "Automatic" mode leaves the VPN Gateway and VPN Client negotiate the NAT-Traversal.
In NAT-T "Forced" mode TheGreenBow IPSec VPN Client will force NAT-T by encapsulating IPSec packets into UDP frames to solve traversal with intermediate NAT routers.

Local ID

Local ID is the identity the VPN Client is sending during Phase 1 to VPN gateway. This identity can be:

- an IP address (type = IP address), for example: 195.100.205.101
- an domaine name (type = DNS), e.g. mydomain.com
- an email address (type = Email), e.g. support@thegreenbow.com
- a string (type = KEY ID), e.g. 123456
- a certificate issuer (type=DER ASN1 DN) (see Certificates configuration) If this identity is not set, VPN Client's IP address is used.

Remote ID

Remote ID is the identity the VPN Client is expecting to receive during Phase 1 from the VPN gateway. This identity can be:

- an IP address (type = IP address), for example: 80.2.3.4
- an domaine name (type = DNS), e.g. gateway.mydomain.com
- an email address (type = Email), e.g. admin@mydomain.com
- a string (type = KEY ID), e.g. 123456
- a certificate issuer (type=DER ASN1 DN) (see Certificates configuration) If this identity is not set, VPN gateway's IP address is used.

X-Auth

Define the login and password of an X-Auth IPSec negotiation. If "X-Auth popup" is selected, a popup window asking for a login and a password will appear each time an authentication is required to open a tunnel with the remote gateway. The end user has 20 seconds to enter its login and password before X-Auth authentication fails.
If X-Auth authentication fails then the tunnel establishment will fail too.

Hybrid Authentication Mode	The Hybrid mode is a specific authentication method used within IKE Phase 1. This method assume an asymmetry between the authenticating entities. One entity, typically an Edge Device (e.g. firewall), authenticates using standard public key techniques (in signature mode), while the other entity, typically a remote User, authenticates using challenge response techniques. These authentication methods are used to establish, at the end of Phase 1, an IKE SA which is unidirectionally authenticated. To make this IKE bi-directionally authenticated, this Phase 1 is immediately followed by an X-Auth Exchange [XAUTH]. The X-Auth Exchange is used to authenticate the remote User. The use of these authentication methods is referred to as Hybrid Authentication mode. TheGreenBow IPSec VPN Client implements the RFC 'draft-ietf-ipsec-isakmp-hybrid-auth-05.txt'.

6.4 IPSec Configuration or Phase 2

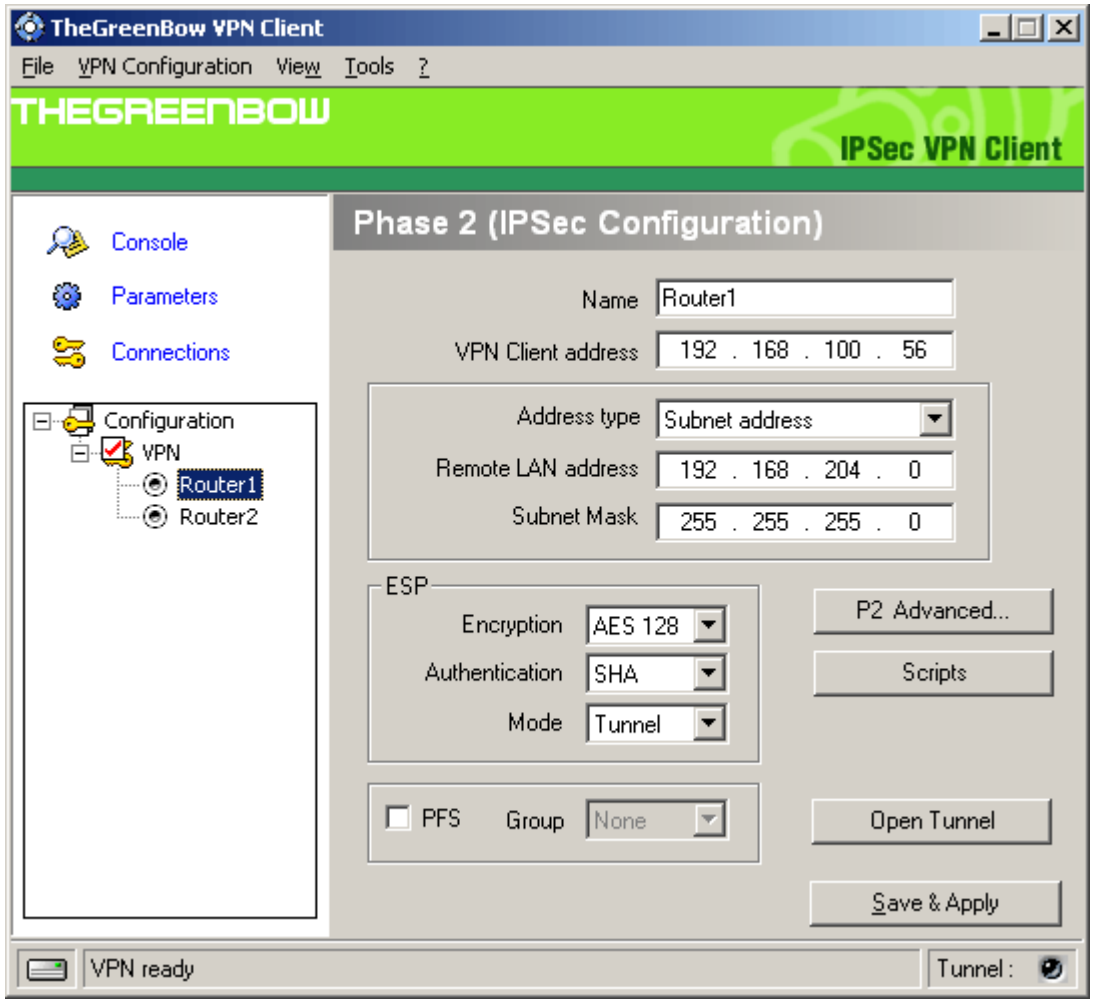
6.4.1 What is Phase 2 ?

'IPSec Configuration' or 'Phase 2' window will concern settings for Phase 2.

The purpose of Phase 2 is to negotiate the IPSec security parameters that are applied to the traffic going through tunnels negotiated during Phase 1.

Property of TheGreenBow© - Sistech SA 2000-2007

6.4.2 Phase 2 Settings Description



Name Label for IPSec Configuration only used by the VPN Client. This parameter is never transmitted during IPSec Negotiation. It is possible to change this name at any time and read it in the tree list window. Two Phases can not have the same name.

VPN Client address Virtual IP address used by the VPN Client inside the remote LAN: The computer will appear in the LAN with this IP address. **It is important this IP address not to belong to the remote LAN (e.g., in the example, you should avoid an IP address like 192.168.1.10).**

Address type The remote endpoint may be a LAN or a single computer,
In case the remote endpoint is a LAN, choose "Subnet address" or "IP Range". When choosing "Subnet address", the two fields "Remote LAN address" and "Subnet mask" become available. When choosing "IP Range", the two fields "Start address" and "End address" become available, enabling TheGreenBow IPSec VPN Client to establish a tunnel only within a range of a predefined IP addresses. The range of IP addresses can be just one IP address.

Incase the remote end point is a single computer, choose "Single Address". When choosing "Single address", only the field "Remote host address" is available.

Remote address This field may be "Remote host address" or "Remote LAN address" depending of the address type. It is the remote IP address, or LAN network address of the gateway, that opens the VPN tunnel.

Subnet mask	Subnet mask of the remote LAN. Only available when address type is equal to "Subnet address".
ESP encryption	Encryption algorithm negotiated during IPSec phase (3DES, AES, ...)
ESP authentication	Authentication algorithm negotiated during IPSec phase (MD5, SHA, ...)
ESP mode	IPSec encapsulation mode: tunnel or transport
PFS group	Diffie-Hellman key length.
Open Tunnel	This button allows to open the tunnel. This button changes to "Close Tunnel" as soon as the tunnel is opened.
Scripts	Scripts may be configured in the Script configuration window.

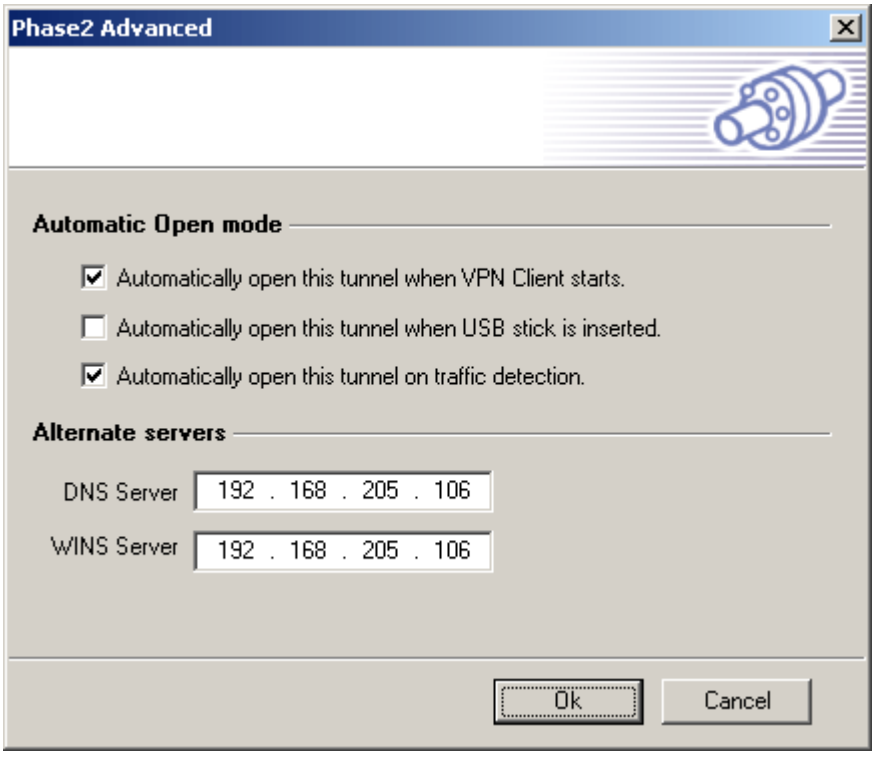
Note: "IP Range" feature combined with "Open tunnel when traffic" feature allows to automatically open tunnel when traffic is detected for a specific range of IP Addresses. However, the range of IP addresses must be authorized in the configuration of VPN gateway.

For more advanced settings, click on 'P2 Advanced'.

Once the parameters are set, click on 'Save & Apply' to save and to take into account the new configuration.
You'll find a set of useful VPN Client configuration documents available for each of the VPN Client gateway we support. Please go to our knowledge base on our website.

6.4.3 Phase2 Advanced Settings Description

For advanced features & parameters, click on 'P2 Advanced' button into Phase2 panel.

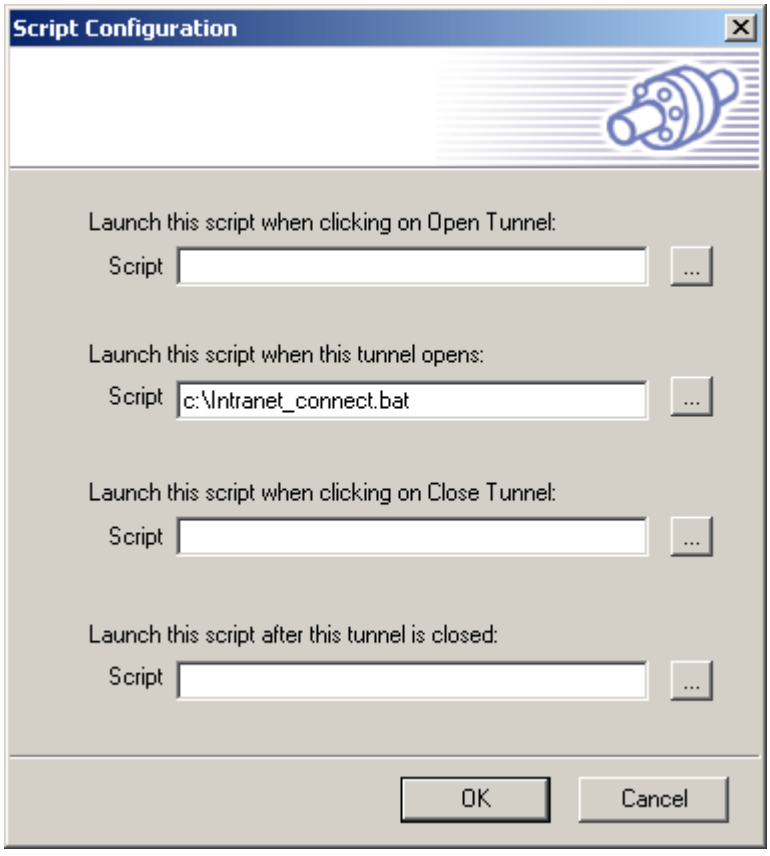

Phase2 Advanced
Automatic Open mode
Automatically open this tunnel when VPN Client starts.
Automatically open this tunnel when USB stick is inserted.
Automatically open this tunnel on traffic detection.
Alternate servers
DNS Server
192 . 168 . 205 . 106
WINS Server
192 . 168 . 205 . 106
Ok
Cancel

Property of TheGreenBow© - Sistech SA 2000-2007

Automatic Open Mode	The VPN Client can automatically open the specified tunnel (Phase2) on specific events such as: • Auto open this tunnel when the VPN Client starts up. • Auto open this tunnel when USB stick is inserted (see section "USB Mode"). • Auto open this tunnel when the VPN Client detect traffic towards remote LAN.
Alternate Servers	DNS ans WINS server IP addresses of the remote LAN can be entered here, to help users to resolve intranet addressing. The DNS or WINS addresses are taken into account as soon as the tunnel is opened, and as long as it is opened.

6.4.4 Script configuration

Scripts may be configured in the Script configuration window. This window can be opened through the button 'Scripts' of a Phase 2 Settings window.



Scripts or applications can be enabled for each step of a VPN tunnel opening and closing process:

- Before tunnel is opened
- Right after the tunnel is opened
- Before tunnel closes
- Right after tunnel is closed

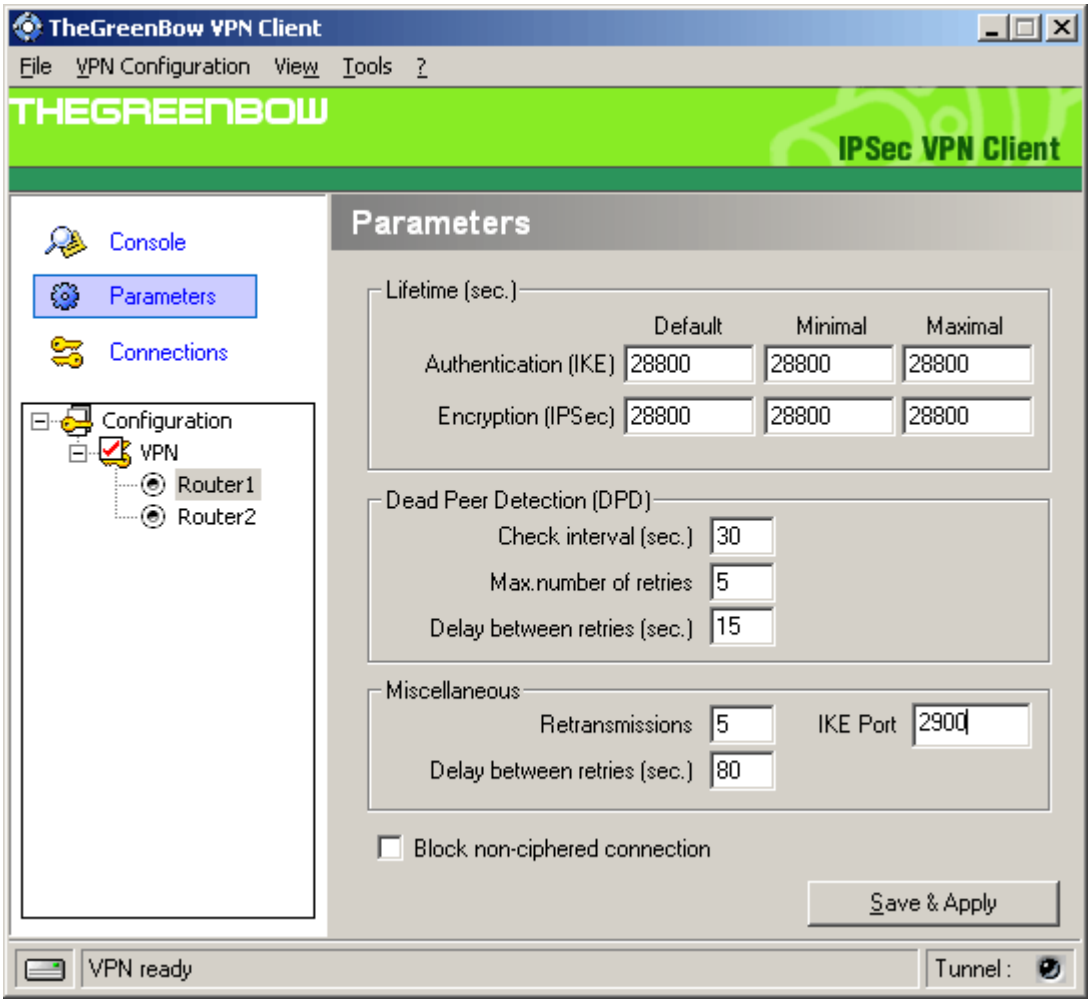
This feature enables to execute scripts (batches, scripts, applications...) at each step of a tunnel connection for a variety of purposes e.g. to check current software release, to check database availability before launching backup application, to check a software is running, a logon is set... .

It also enables to configure various network configuration before, during and after tunnel connections.

6.5 Global Parameters

6.5.1 Global Settings Description

Global Parameters are generic settings that apply to all created VPN tunnels. Once modified, click on 'Save&Apply' to take into account your modifications.



- **Lifetime (sec.)**
  - **IKE default lifetime** — Default lifetime for IKE rekeying.
  - **IKE minimal lifetime** — Minimal lifetime for IKE rekeying.
  - **IKE maximal lifetime** — Maximal lifetime for IKE rekeying.
  - **IPSec minimal lifetime** — Default lifetime for IPSec rekeying.
  - **IPSec maximal lifetime** — Maximal lifetime for IPSec rekeying.
  - **IPSec minimal lifetime** — Minimal lifetime for IPSec rekeying.
- **Dead Peer Detection (DPD)**
  - **Check interval (sec.)** — Interval between DPD messages.
  - **Max number of retries** — Number of DPD messages sent.
  - **Delay between retries (sec.)** — Interval between DPD messages when no reply from remote gateway.
- **Miscellaneous**
  - **Retransmissions** — How many times a message should be retransmitted before giving up.

Property of TheGreenBow© - Sistech SA 2000-2007

Delay between retries	Minimum time before any attempts by user to restart IKE negotiation.
Block non-ciphered connection	When this option is checked, only encrypted traffic is authorized.
IKE Port	User can change port number for IKE negotiation. Exchanges are still on UDP but they can be on another port than 500 as some firewalls do not allow IKE Port 500. The remote gateway must support this feature.

Dead Peer Detection (i.e. DPD) is an Internet Key Exchange (IKE) extension (i.e. RFC3706) for detecting a dead IKE peer. TheGreenBow IPSec VPN Client is using DPD:

- to delete opened SA in the VPN Client when peer has been detected dead.
- to re-start IKE negotiations with the Redundant Gateway if activated in the 'Phase1 Advanced' Configuration Panel.

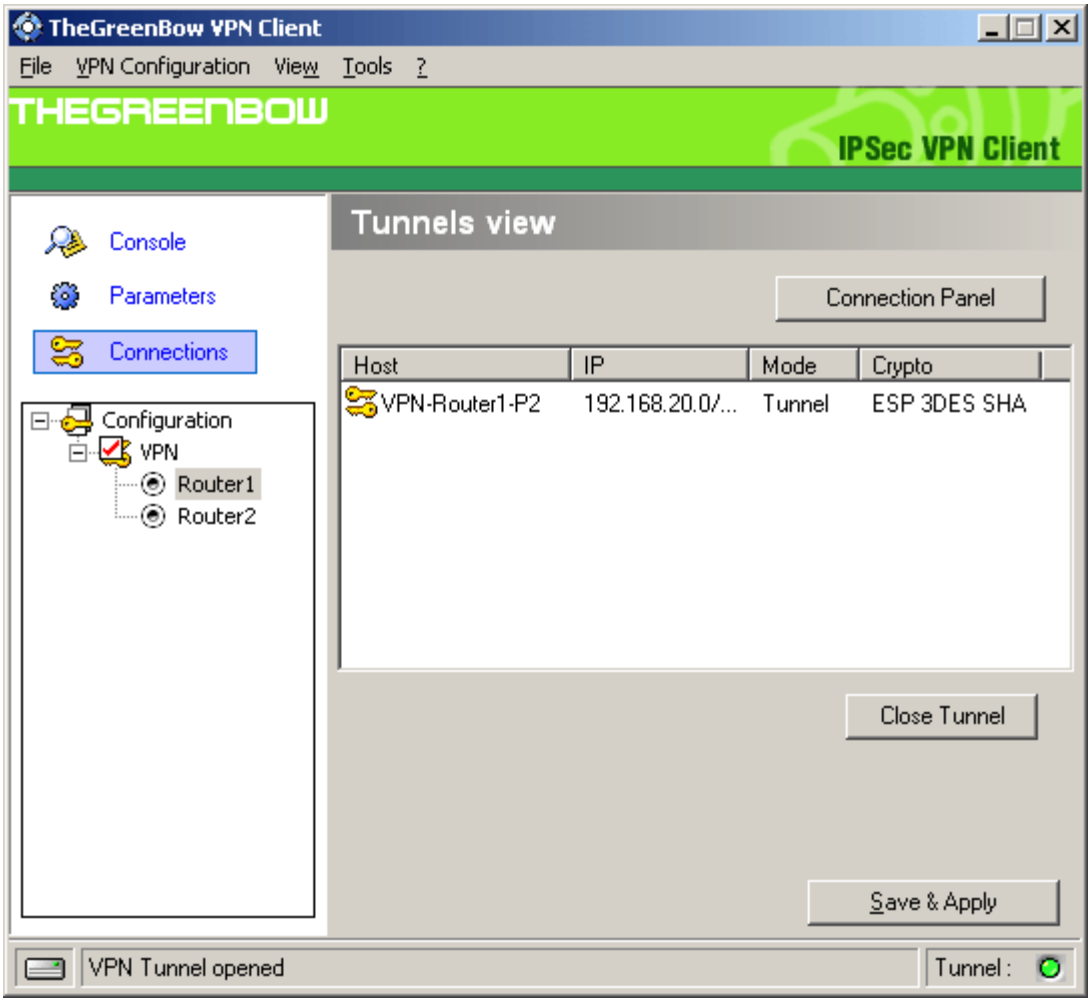
Once the parameters are set, click on 'Save & Apply' to save and to take into account the new configuration.

6.6 VPN Tunnel View

6.6.1 How to view opened tunnels ?

'Tunnel View' screen shows VPN tunnels currently opened This screen may also be used to close opened tunnels. To close a VPN tunnel, select the tunnel in the list and click on 'Close Tunnel'. Tunnels may also be viewed, opened and closed directly from the context menu of the system tray icon.

Property of TheGreenBow© - Sistech SA 2000-2007



6.7 USB Mode

6.7.1 What is USB Mode ?

TheGreenBow VPN Client brings the capability to secure VPN configurations and VPN security elements (e.g. PreShared key, Certificates, …) by the use of an USB Stick.

When you select "USB mode", the VPN configuration and security elements contained into the configuration are stored onto the USB Stick the first time you plug it in.

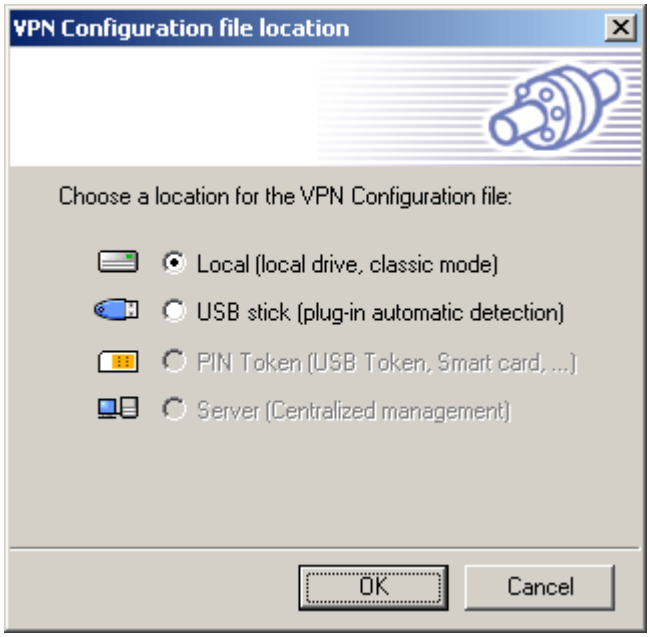
Once done, you just need to insert the USB Stick to automatically open tunnels. And you just need to unplug the USB Stick to automatically close all established tunnels.

6.7.2 How to set USB Mode ?

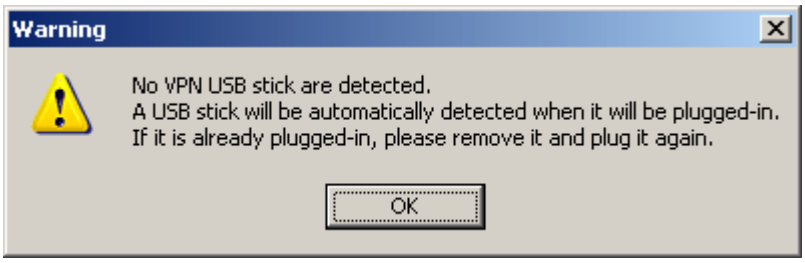
The USB Mode can be set by clicking on the 'USB Stick' icon in the status bar of the Configuration Panel or via the menu:

- Select menu 'File' > 'VPN Configuration File...'
- Select 'USB Stick'

Property of TheGreenBow© - Sistech SA 2000-2007


VPN Configuration file location
Choose a location for the VPN Configuration file:
Local (local drive, classic mode)
USB stick (plug-in automatic detection)
PIN Token (USB Token, Smart card, ...)
Server (Centralized management)
OK
Cancel

Note: At this stage, if an USB Stick containing a VPN configuration with VPN security elements is already plugged in, the associated drive will be automatically recognized. Please note also that this is not necessary to insert a USB Stick during this step. In case no USB Stick is plugged in, the following pop window will inform the user:


Warning
No VPN USB stick are detected.
A USB stick will be automatically detected when it will be plugged-in.
If it is already plugged-in, please remove it and plug it again.
OK

Once USB mode is set on, the left side box in the status bar shows an USB stick icon.

The USB Stick icon is plain when a USB Stick is plugged in:

The USB Stick icon is gray when no USB Stick is plugged in:

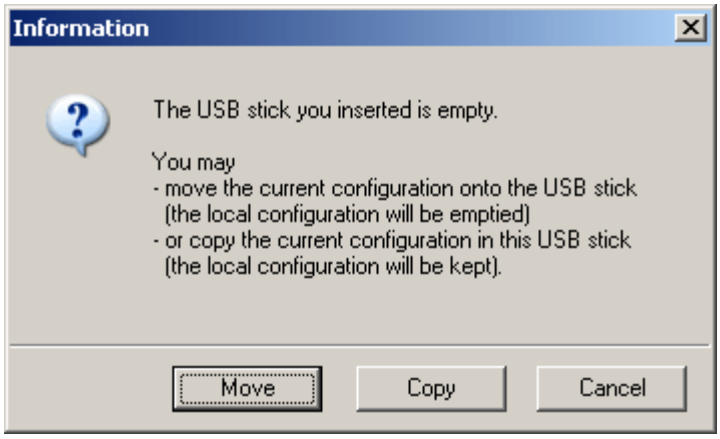
6.7.3 How to enable a new USB Stick ?

A new USB Stick (no data) is enabled by copying VPN configuration and security elements onto it.

When you insert a new USB Stick, the IPSec VPN Client automatically propose to enable the USB Stick through the following options:

- **Copying** the VPN configuration and security elements onto the USB Stick: the VPN Client will copy the security information onto the USB Stick and leave a copy in the computer. This feature is specially designed for IT Managers to enable multiple USB Sticks for multiple users in no time.
- **Moving** the configuration onto the USB Stick: the IPSec VPN Client will copy the security information onto the USB Stick and remove all security information from the computer. This method is used to secure a computer once VPN configuration completed setup.

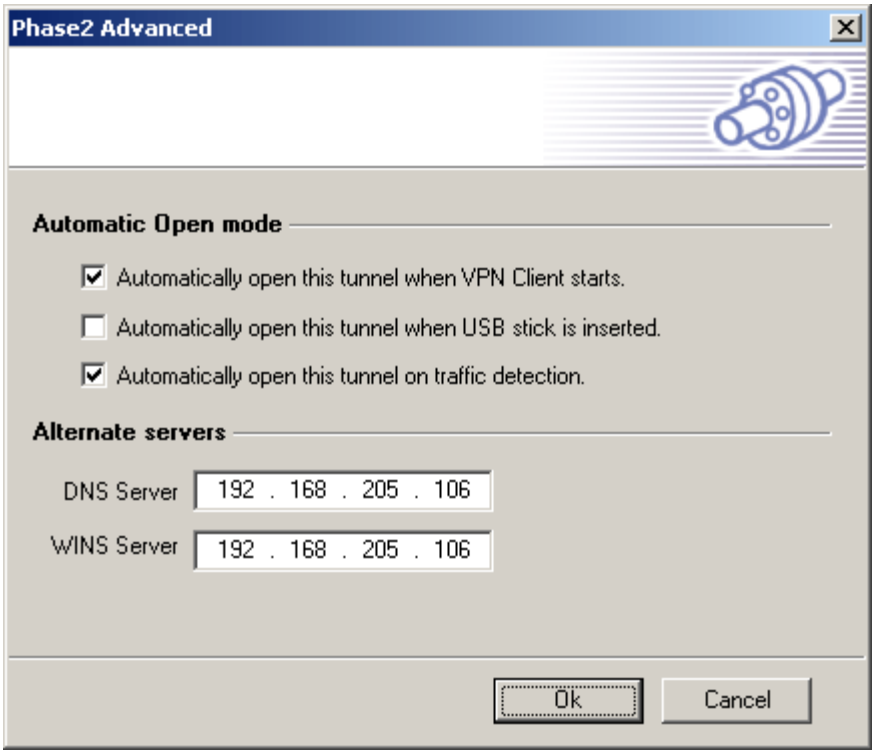
Property of TheGreenBow© - Sistech SA 2000-2007


Information
The USB stick you inserted is empty.
You may
- move the current configuration onto the USB stick
(the local configuration will be emptied)
- or copy the current configuration in this USB stick
(the local configuration will be kept).
Move
Copy
Cancel

6.7.4 How to automatically open tunnels when an USB Stick is plugged in ?

Each and every tunnels may be configured individually:

- In the IPSec Configuration (Phase 2) of the relevant tunnel, click on 'P2 Advanced' button
- Select the 'Automatically open this tunnel when USB stick is inserted' mode


Phase2 Advanced
Automatic Open mode
Automatically open this tunnel when VPN Client starts.
Automatically open this tunnel when USB stick is inserted.
Automatically open this tunnel on traffic detection.
Alternate servers
DNS Server
192 . 168 . 205 . 106
WINS Server
192 . 168 . 205 . 106
Ok
Cancel

6.8 Certificate Management

6.8.1 Certificate Management overview

TheGreenBow IPSec VPN Client can use Certificates from PEM files, PKCS#12 file or SmartCard.

Property of TheGreenBow© - Sistech SA 2000-2007

Note: TheGreenBow VPN Client doesn't allow to create Certificates. Certificates must be created (and stored on SmartCard) by third party software. You'll find additional support documents on "How to generate Certificates" or "How to convert Certificate formats" on our website.

When used by TheGreenBow IPSec VPN Client, it is composed of the following items:

- Root certificate
- User certificate
- Private key of the user certificate

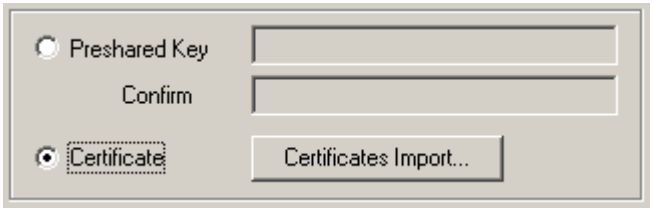
Note: This feature makes management the VPN configurations easier, since a full VPN Configuration (including Certificates) can be provided and quickly implemented by end-users.

6.8.2 How to configure IPSec VPN Client with PKCS#12 Certificates

PKCS#12 certificates are supported by a lot of gateways. TheGreenBow IPSec VPN Client can import PKCS#12 certificates into the VPN Configuration, directly from the main interface. One PKCS#12 certificate can be defined per tunnel. Therefore, it is possible to connect to several gateways that do not use the same PKI (Public Key Infrastructure).

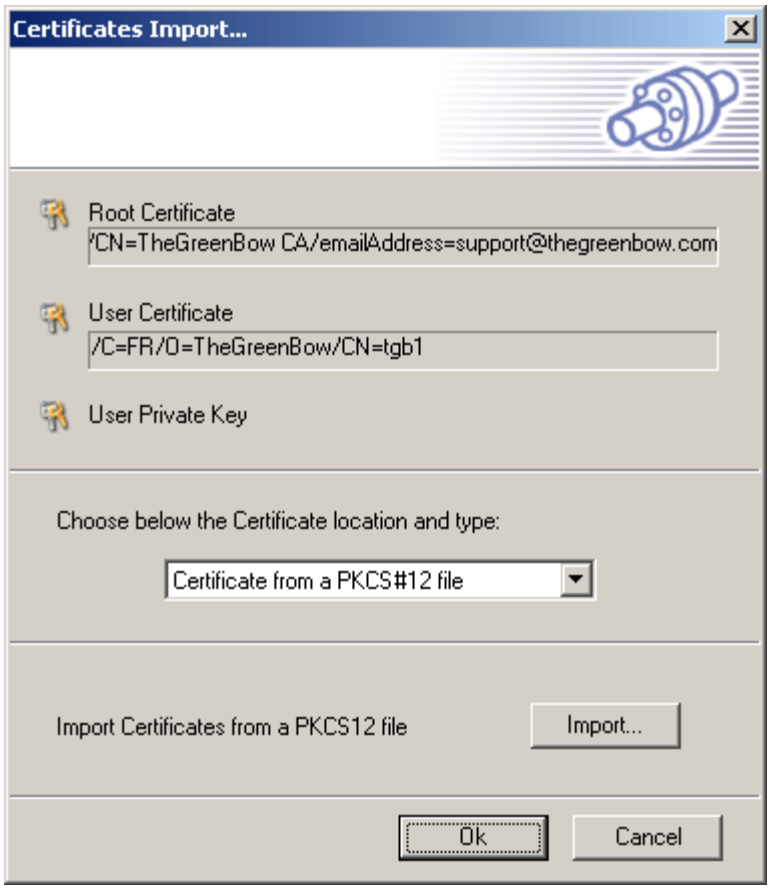
Here are the steps to configure the IPSec VPN Client with **PKCS#12 Certificates**:

Step 1: Select radio button 'Certificate' in the 'Phase 1' window and click on 'Certificates Import...'



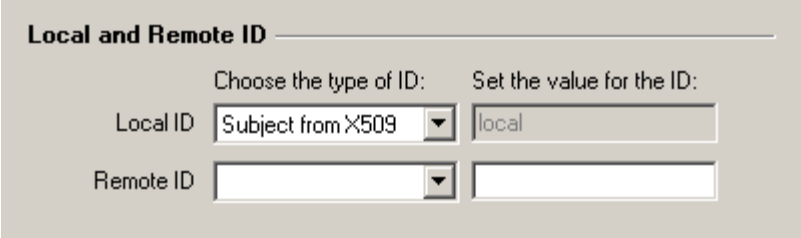
Step 2: Select 'Certificate from a PKCS#12 file' in the list box, then click on the 'Import...' button

Step 3: Select the PKCS#12 Certificates you want to import. If the PKCS#12 Certificate is protected, enter the password in the password pop up window. Once the Certificate is correctly imported, its subject is automatically displayed in the top fields of the 'Certificates Import ...' window. Also, key icons are displayed next to each certificate component (root certificate, user certificate, private key) as shown below.



Step 4: PKCS#12 Certificates will be stored in the VPN Configuration file as soon as you click on "Save&Apply".

Note: Once the Certificate is imported, its subject is used for the local ID of the associated Phase1. This is shown in the P1 Advanced window with the following indication:

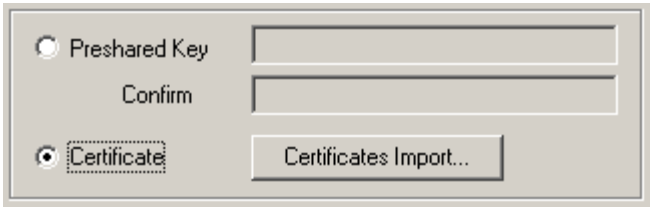


6.8.3 How to configure IPSec VPN Client with PEM Certificates

TheGreenBow IPSec VPN Client can import PEM Certificates into the VPN Configuration, directly from the Configuration Panel. One PEM Certificate can be defined per tunnel. Therefore, it is possible to connect to several gateways that do not use the same PKI (Public Key Infrastructure).

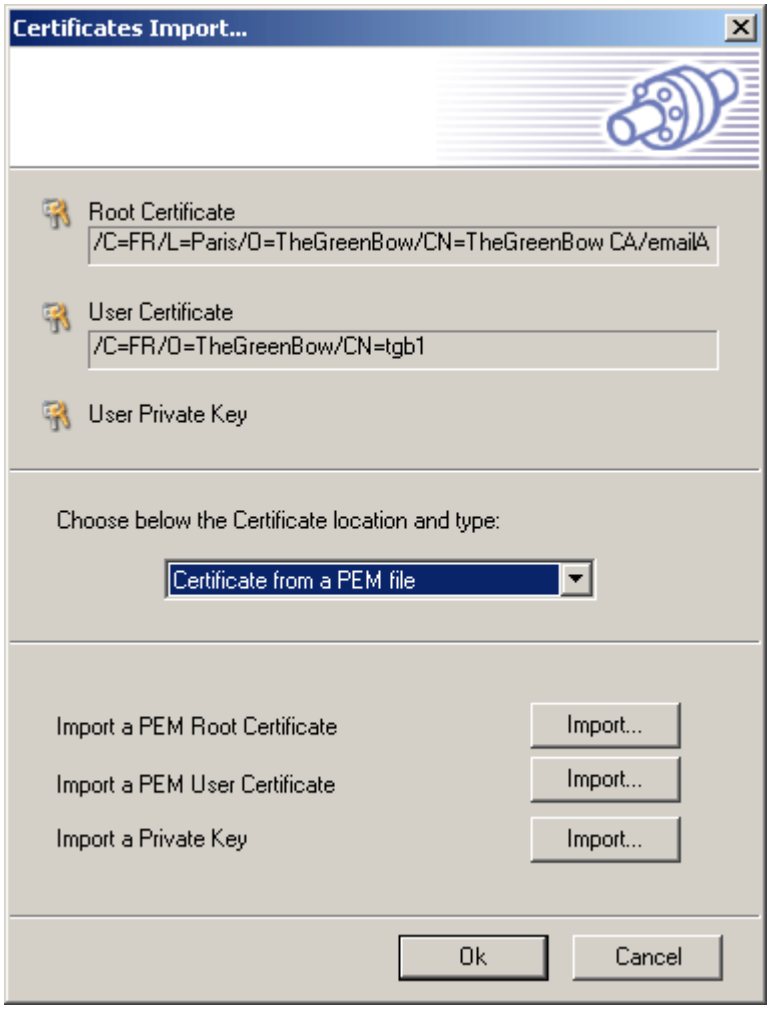
Here are the steps to configure the IPSec VPN Client with PEM Certificate

Step 1: Select radio button 'Certificate' in the Phase 1 window and click on 'Certificates import...'



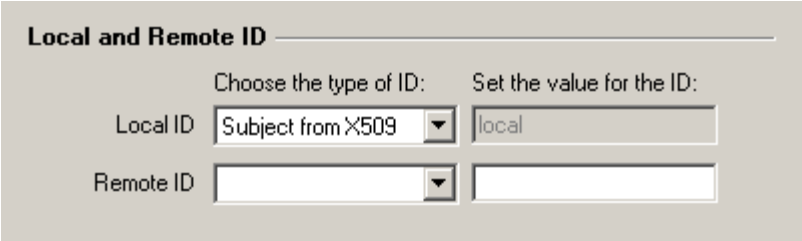
Step 2: Choose "Certificate from a PEM file" in the list box

Step 3: Import the Root Certificate, the User Certificate and the Private Key by clicking on the associated button. Once the certificate is correctly imported, its subjects are filled in the 'Certificate Import...' window.



Step 4: PEM Certificates will be stored in the VPN Configuration file as soon as you click on "Save&Apply".

Note: Once the Certificate is imported, its subject is used for the local ID of the associated Phase1. This is shown in the P1 Advanced window with the following indication:



Note : The PEM file enclosing the private key must not be encrypted or protected with a password.

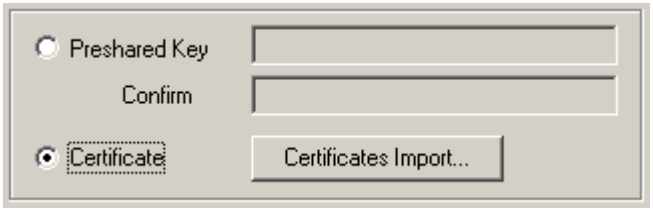
6.8.4 Smart Card and Token Management

6.8.4.1 How to configure a tunnel with Certificates from a SmartCard

TheGreenBow IPSec VPN Client can read Certificates from Smart Cards. Smart Cards can be used for securing X509 certificates that can be protected by a PIN code.

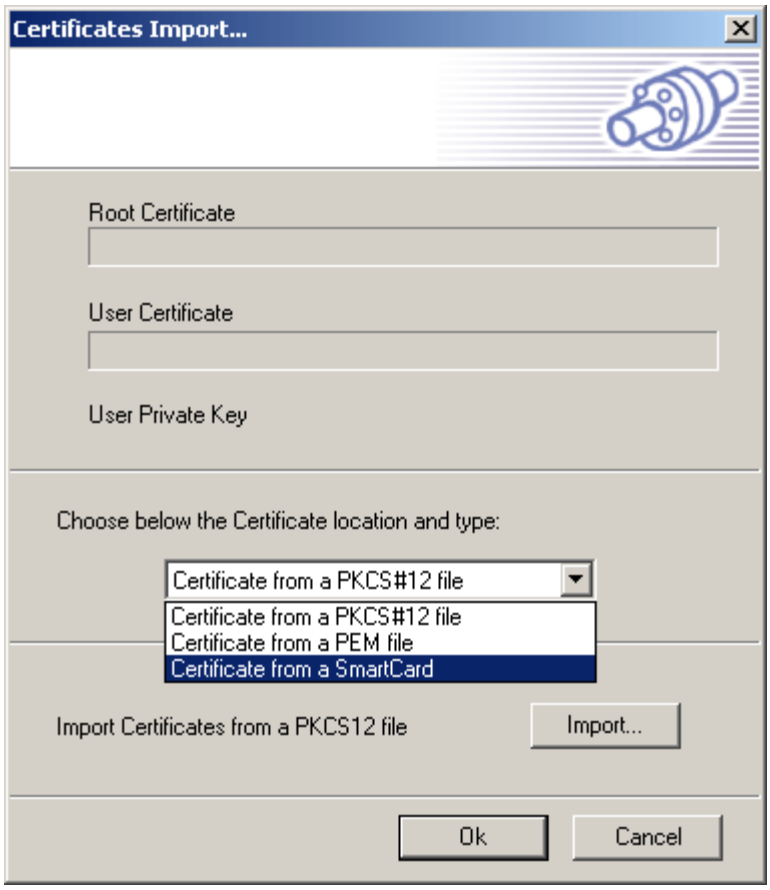
Here are the steps to configure a tunnel using Certificates from Smart Cards:

Step 1: Select radio button 'Certificate' in the 'Phase 1' window and click on 'Certificates Import...'

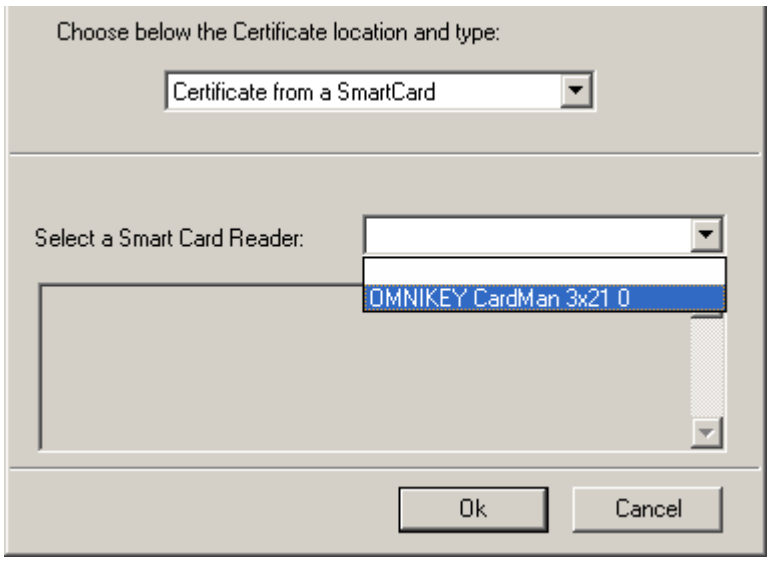


Step 2: Select 'Certificate from a SmartCard' in the list box. The bottom part of the window shows a list of SmartCard Reader.

Property of TheGreenBow© - Sistech SA 2000-2007

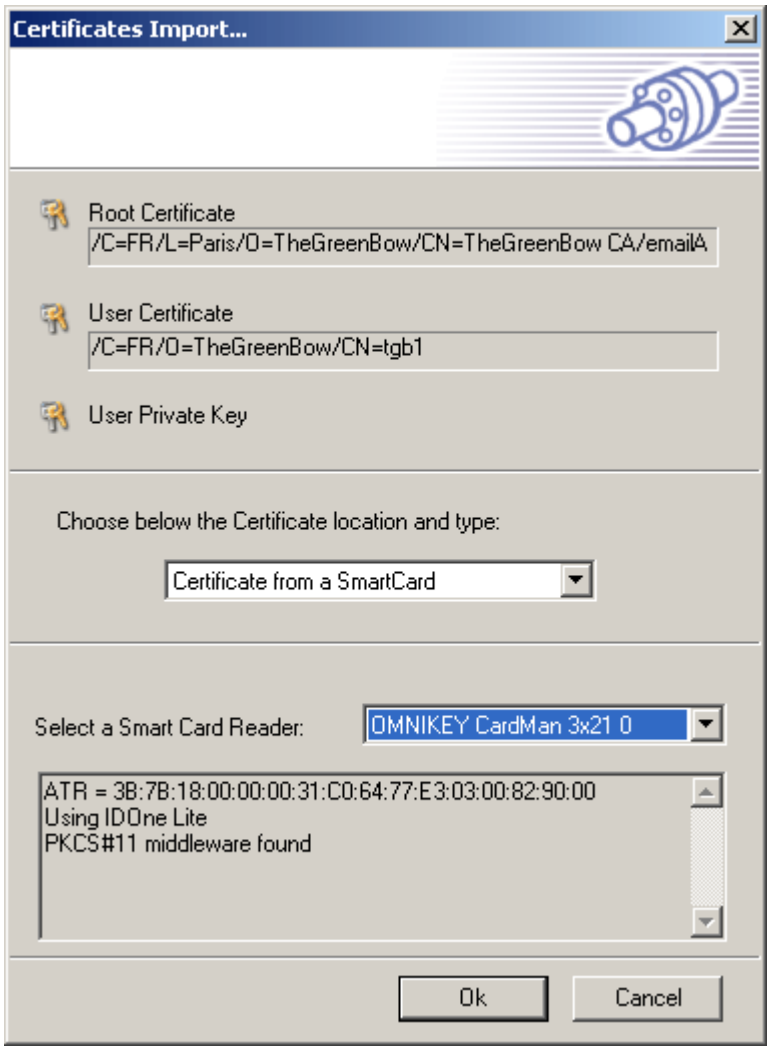


Step 3: Select the SmartCard Reader you want to use. The SmartCard Reader identification process starts and a PIN code may be required. Enter your 'SmartCard PIN code' and click 'OK'.



Once the SmartCard is successfully read, information about the SmartCard Reader and the SmartCard are displayed in the text area below the list box, while the subjects of the Certificates are displayed in the top two fields of the window:

Property of TheGreenBow© - Sistech SA 2000-2007



Step 4: SmardCard Reader information will be stored in the VPN Configuration file as soon as you click on "Save&Apply".

.

6.8.4.2 How to use a tunnel with Certificates from a SmartCard

When a tunnel is configured to use Certificates from a SmartCard, the PIN code of the SmartCard is asked to the user each time the tunnel must be opened (excepted on automatic VPN renegociations).

Thus, to open a tunnel with Certificates from a SmartCard, it is required to have :

1. The SmartCard reader correctly installed and configured in the IPSec VPN Client
2. A readable SmartCard inserted in the SmartCard reader
3. The correct PIN code for reading the SmartCard.

Each issues while using SmartCard is displayed in the Software Console. See section 'SmartCard TroubleShooting' below.

6.8.4.3 SmartCard Troubleshooting

Users may encounter issues while configuring SmartCard and SmartCard Readers.

SmartCard Trouble	Message displayed (*)

Property of TheGreenBow© - Sistech SA 2000-2007

No SmartCard Reader is found
If no SmartCard is found, it is probably because the SmartCard Reader middleware is missing. The procedure to easily add a SmartCard Reader middleware is displayed in the text area below the list box.
	`No smart card found`
	`No ATR`
	`Unknown ATR: this smart card may not be supported.`
	`No PKCS#11 middleware for this smart card was found.`
	`You can set PKCS#11 middleware with the command line :`
	`Vpnconf.exe /addmiddleware:path_to_the_dll`

The SmartCard cannot be read	`ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00`
	`Using IDOne Lite`
	`PKCS#11 middleware found`
	`Error 0x00000015`

The PIN code is wrong	`ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00`
	`Using IDOne Lite`
	`PKCS#11 middleware found`
	`Wrong PIN code`

No certificate can be found in the SmartCard	`ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00`
	`Using IDOne Lite`
	`PKCS#11 middleware found`
	`No configuration or no certificate found in the smart card`

(*) Message displayed in the text area below the SmartCard listbox.

Users may encounter issues while opening a tunnel which requires Certificates on a SmartCard.

Smart Card Trouble	Message displayed in the Console.
No SmartCard Reader is found	`Missing SmartCard Reader`
The PIN code is wrong	`Wrong PIN code`
no certificate can be found in the SmartCard or The SmartCard cannot be read	`Empty or unreadable SmartCard`

6.9 Configuration Management

6.9.1 Import or Export VPN Configuration via menu

TheGreenBow VPN Client can import or export a VPN Configuration. With this feature, IT managers can prepare a configuration and deliver it to other users.

- Importing a configuration, select menu "File > Import VPN Configuration".
- Exporting a configuration, select menu "File > Export VPN Configuration".

All configuration files will have a ".tgb" extension.

VPN Configuration including Certificates can be protected by a password during import or export. When the user wants to export a configuration, a window automatically asks if the exportated VPN configuration must be protected with a password or not.

Property of TheGreenBow© - Sistech SA 2000-2007

Export Protection
You are about to export a VPN Configuration.
You may protect this configuration with a password.
It will be automatically asked to the user when imported.
Don't protect the exported VPN Configuration
Protect the exported VPN Configuration
Enter the password :
OK
Cancel

When a VPN Configuration is protected with a password, its importation will automatically ask the user to enter the password. An exported VPN Configuration which is not protected with a password will be automatically imported without any request to the user.

Note: Import/Export in 'USB Mode'
When the VPN Client is configured in "USB Mode" and when a USB stick is inserted, the importation of a VPN Configuration is directly written on the USB stick. If the VPN Client is configured in "USB mode" but no USB stick is inserted (the USB icon in the bottom left corner of the GUI is disabled), the exportation and importation of a VPN Configuration are disabled.

Note: A VPN Configuration file can also be imported via the command line.

6.9.2 Embed your own VPN Configuration into IPSec VPN Client Setup

A (pre-created) VPN Configuration may be enclosed into the IPSec VPN Client Setup. Enclosing VPN Configuration within the IPSec VPN Client Setup enables IT Manager to deploy pre-configured IPSec VPN Client software in a single package to all company users.

6.9.3 Default VPN Configuration

The IPSec VPN Client Setup embeds a Default VPN Configuration. This Default VPN Configuration enables to open a tunnel to our TheGreenBow Demo Server as soon as the IPSec VPN Client software is installed.

It is particularly useful to check if a tunnel can be opened from my computer to an operational remote network for test – and eventually for debug – purpose.

Property of TheGreenBow© - Sistech SA 2000-2007

Part VII

Deployment

7 Deployment

7.1 Embedded VPN Configuration

A VPN Configuration ".tgb" file embedded within the IPSec VPN Client Setup (unzipped, see 'Deployment Guide' description on our website) is automatically imported by the IPSec VPN Client during software installation.

The process to create a setup with a VPN Configuration is the following:

1. Create the VPN Configuration that need to be embedded into the Setup. This step must be processed from a formerly installed IPSec VPN Client, from which the VPN Configuration is exported and named 'myconfig.tgb'.
2. Create a silent installation, or simply unzip the IPSec VPN Client Setup.
3. Add the VPN Configuration "'myconfig.tgb" file into the unzipped setup directory.
4. Deploy the package to the user (the "'myconfig.tgb" VPN Configuration will be used during the setup)

Important note: the Setup cannot import and use an encrypted (protected) VPN Configuration. When creating your VPN Configuration make sure it is exported without being encrypted (without being protected with a password).

7.2 Setup options

7.2.1 Setup option overview

Several options are available with the IPSec VPN Client Setup.

1. Configuration of the GUI mode: *'full'*, *'user'* or *'hidden'*
2. Protection of the GUI mode access control with a password
3. Configuration of the systray menu items.
4. Other options for Software Start, License Number and Activation email

7.2.2 Setup option for GUI mode

Syntax: **`--vpngui=full|user|hidden`**
enables to define the GUI appearance when the IPSec VPN Client starts.

"**`full`**": [Default] The Configuration Panel is displayed.
"**`user`**": The Connection Panel is displayed.
"**`hidden`**": Both VPN Configuration Panel and Connection Panel are not displayed. Only the systray menu can be opened. Tunnels can be opened from the systray menu.

Remark:
`--vpngui=hidden` is equivalent to option **`--hide=yes`**. This option can still be used (as it is maintained for compatibility reasons).

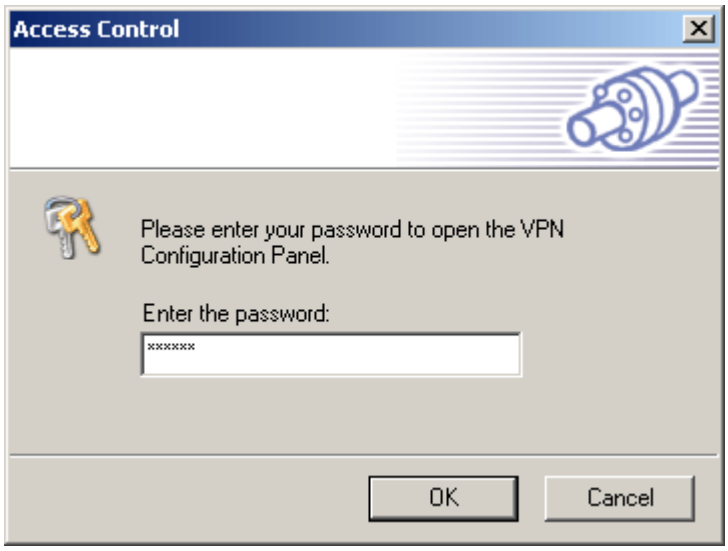
7.2.3 Setup option for GUI mode access control

Syntax: **`--password=mypwd`**
Enables to control the acces to the VPN GUI with a password.

The user will be asked for the password:

- When the user clicks or double-clicks on the VPN systray icon
- When the user wants to switch from the Connection Panel to the Configuration Panel.

Property of TheGreenBow© - Sistech SA 2000-2007



Example: **--vpngui=user --password=admin01**
These 2 options enable the GUI to be locked in "Connection Panel" mode only, while the access to the Configuration Panel is protected with a password.

7.2.4 Setup option for systray menu items

Syntax: **--menuitem=[0...15]**
Enables to specify the items of the systray menu that the IT manager wants to keep.

The value is a 'bitfield': **1 = Quit**, **2 = Connection Panel**, **4 = Console**, **8 = Save & Apply**.

Example: **--menuitem=5** will configure a systray menu with the items: Quit + Console.

Note 1: the tunnels are always shown in the systray menu, and can always be opened and closed from this systray menu.

Note 2: **'menuitem'** and **'vpngui=hidden'**.
By default, **vpngui=hidden** (or **hide=yes**) set the systray menu item list to Quit + Console. (The items 'Save&Apply' and 'Connection Panel' are not visible). However the use of **'menuitem'** overrides **'vpngui'**.
That means the following: "**--vpngui=hidden --menuitem=1**" will set a systray menu with only the 'Quit' item.

7.2.5 Other Setup options

Here are the other installation parameters for the setup command line:
Syntax: **-s**
Allows to install in a silent mode.

Syntax: **--license=[licence_number]**
Allows to configure the licence number. The License Number is a set of 24 hexadecimal characters. Old License Numbers might be 20 hexadecimal characters.

Syntax: **--start=[logon|boot|manual]**
Allows to configure the start mode for the VPN Client: after the logon windows, during the boot, or manually. Default is [logon].

Property of TheGreenBow© - Sistech SA 2000-2007

Syntax: **--activmail=[activation_email]**
Allows to force the email used for activation confirmation. During the activation process, the edit box used for entering this email will be disabled

> Warning: the switches '**--license**', '**--start**', '**--activmail**' can only be used with the switch '**-s**' (silent mode).

Example:
Setup -s --license=0123456789ABCDEF0123 --start=boot --activmail=smith@smith.com

7.3 Command line

7.3.1 Command line options

Several configuration tools are available on our web site. Those tools are available as command line type and are meant to be used by IT managers to change the IPSec VPN Client behavior to their needs.

- Stopping IPSec VPN Client
- Import or Export VPN Configuration

7.3.2 Stopping IPSec VPN Client: option "/stop"

TheGreenBow VPN Client can be stopped at any time by the command line:

" **[path]\vpnconf.exe /stop** " where **[path]** is the IPSec VPN Client installation directory.

If there is several active tunnels, they will close properly.

This feature can be used, for example, in a script that launch the VPN Client after establishing a dialup connection and exit it just before the disconnection.

7.3.3 Import VPN Configuration options

TheGreenBow VPN Client can import a specific configuration file by the command line:
" **[path]\vpnconf.exe /import:[file.tgb]** " where **[path]** is the VPN Client installation directory, and **[file.tgb]** is the VPN Configuration file. This command doesn't handle relative paths (e.g. "..\..\file.tgb").

" **/import:** " may be used either if the VPN Client is running or not. When the VPN Client is already running, it imports dynamically the new configuration and automatically applies it (i-e: restarts the IKE service). If the VPN Client is not running, it is launched with the new configuration.

" **/importonce:** " allows to import a VPN configuration file without running the VPN Client. This command is especially useful in installation scripts: it allows to run a silent installation and to import a configuration automatically.

" **/export:** " exports the current VPN Configuration (including certificates) in the specified file. This command runs the VPN Client if it is not already running. This command doesn't handle relative paths (e.g. "..\..\file.tgb").

" **/exportonce:** " Exports the current VPN Configuration (including certificates) in the specified

file. This command doesn't run the VPN Client if it is not running.

All 4 arguments "**`import`**", "**`importonce`**", "**`export`**" and "**`exportonce`**" are exclus es and cannot be used together.

Property of TheGreenBow© - Sistech SA 2000-2007

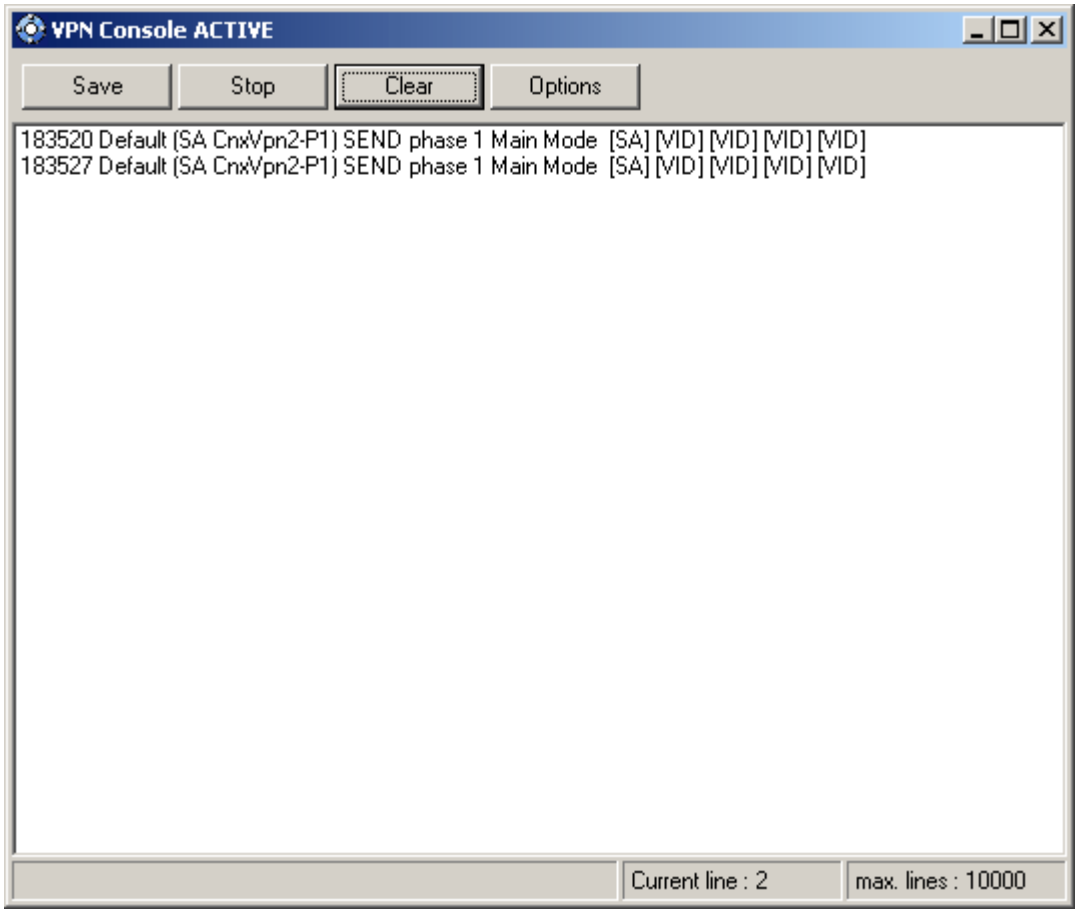
Part VIII

Console and Logs

8 Console and Logs

8.1 Console Windows

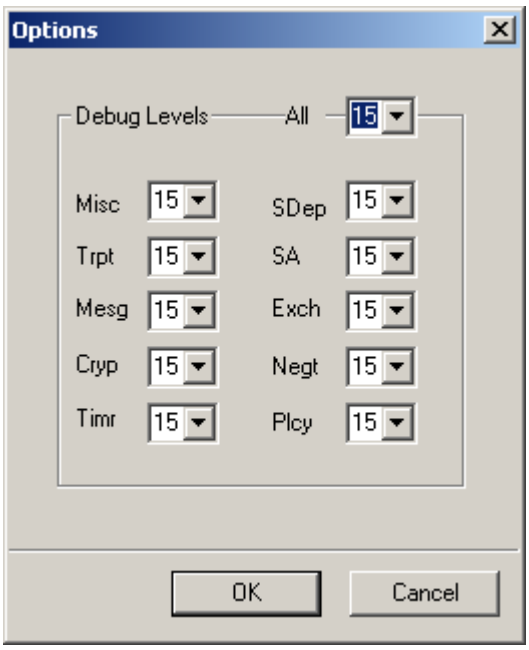
The 'Console' window is available from the context menu of the systray icon or from 'Console' button in the configuration user interface. This window can be used to analyze VPN tunnels. This tool is particularly useful for IT managers in setting up their network.


VPN Console ACTIVE
Save
Stop
Clear
Options
183520 Default (SA CnxVpn2-P1) SEND phase 1 Main Mode [SA] [VID] [VID] [VID] [VID]
183527 Default (SA CnxVpn2-P1) SEND phase 1 Main Mode [SA] [VID] [VID] [VID] [VID]
Current line : 2
max. lines : 10000

Button	Description
Clear	Clear console window content
Save	Save logs in a file
Stop	Stop saving logs in a file
Options	Set level of log filtering

Property of TheGreenBow© - Sistech SA 2000-2007

8.2 Console Filters



Label	Name	Description
Misc	Misc	log level for configuration reading or dump of low level messages
Trpt	Transport	log level for UDP transport mode
Mesg	Message	log level for IKE decode
Cryp	Crypto	log level and dump for crypto material exchanged
Timr	Timer	log level about timers
SDep	Sysdep	log level about IKE interface from/to IPSec
SA	SA	log level for SA managment
Exch	Exchange	log level about IKE exchanges (very useful)
Negt	Negotiation	log level about phase 1 and phase 2 negociation
Plcy	Policy	not used
All	All	Apply the same log level to all subsystems

Most of the time log level set to 0 is largely enough for resolving configuration issues.

Property of TheGreenBow© - Sistech SA 2000-2007

Part IX

Software Localization

9 Software Localization

The localization (L10N) of the IPSec VPN Client is now possible, even by a third party company. All the strings used by the VPN Client are listed in a Translation tool, ready for translation.

Step1: Download the VPN Client Translation tool from our website.
Step2: Translate the strings into your own language
Step3: Send us back the translated VPN Client string file to: support@thegreenbow.com
Step4: We will include your language into the next Generally Available (GA) Product release of the IPSec VPN Client. See on our website who is contributing already.

The whole translation process is also described at www.thegreenbow.com/vpn_local.html.

Property of TheGreenBow© - Sistech SA 2000-2007

Part

Contacts

10 Contacts

Information and update are available at: www.thegreenbow.com
Technical support by email at: support@thegreenbow.com
Sales support by email at: sales@thegreenbow.com

Property of TheGreenBow© - Sistech SA 2000-2007

Index

- A -

About 20
Activation errors 10
Activation Wizard 9

- C -

Certificate from PEM file 45, 47
Certificate from PKCS#12 file 45, 46
Certificate from SmartCard 45
Certificate Management 45, 46, 47
Command line 57
Configuration Panel 19
Configuration Wizard 30, 31, 32
Configuration Wizard to create VPN tunnels 30
Connection Panel 23, 26, 27
Console 60
Console Filters 61

- D -

Default VPN Configuration 53

- E -

Embed VPN Configuration 53
Evaluation period 6
Export VPN Configuration 52

- F -

Features 2

- G -

Global parameters 41

- H -

Hidden user interface 21
How to automatically open tunnels when an USB Stick is plugged in ? 45
How to create a VPN Tunnel ? 32
How to enable a new USB Stick ? 44
How to install ? 6
How to set USB Mode ? 43
How to view opened tunnels ? 42

- I -

IKE Port 41
Import Command line 57
Import VPN Configuration 14, 52
Import with double click on VPN Configuration icon 14

- L -

License Number 9
Linux appliance compatibility 2
Localization 63

- M -

Maintenance 11
Menu 19
Multi Gateway Compatibility 2

- O -

OEM Partners 4

- P -

PEM 45, 47
Phase1 Advanced Settings 35
Phase1 Settings 34
Phase2 Advanced Settings 39
Phase2 Settings 38
PKCS#12 45, 46
Preferences 23
Proxy 9

- R -

RDP session 2
Remote Desktop 2

- S -

Sales contact 65
Script 40

Property of TheGreenBow© - Sistech SA 2000-2007

Setup 53
Setup options 55, 56
Shortcut 18
SmartCard Troubleshooting 51
Software Activation 9, 10
Software upgrade 11
Status Bar 20
Stop software 57
Support contact 65
System tray icon 18

- T -

Temporary Software License 7

- U -

Uninstall 12

- V -

VPN Configuration 52, 53, 55, 57
VPN Configuration with Certificates 46, 47

- W -

What is IKE Phase 1 ? 33
What is IKE Phase 2 ? 37
What is USB Mode ? 43
What's the IPSec VPN Client for ? 2
Wizard 22

Property of TheGreenBow© - Sistech SA 2000-2007

Secure, Strong, Simple.

TheGreenBow Security Software

Property of TheGreenBow© - Sistech SA 2000-2007